Taking Down Telecommunications

GERALD R. HUST, Major, USAF
School of Advanced Airpower Studies

Contents

Abstract

Information is one of the most, if not the most, essential element of combat capability. Because telecommunications affects every aspect of a society, and is probably the most important medium which military information is exchanged, this thesis provides an understanding of the telecommunications system and how best to exploit it across the spectrum of conflict. I examine the system's vulnerabilities to both lethal and nonlethal attack mechanisms. While the ability to employ nonlethal technologies are currently limited, I recommend pursuing a strong research and development program to acquire this capability. The reason is that they provide additional policy options to deal with conflict, they are cheap, and because research may not only discover unanticipated capabilities for the US, but also identify countermeasures to protect our own systems. This thesis concludes by offering guidelines to help determine whether to exploit telecommunications with either lethal or nonlethal attack strategies.

About the Author

Maj Gerald R. Hust was commissioned from the United States Air Force Academy in 1977. After completing Undergraduate Navigator Training, he accumulated 2300 hours in the F-111A, E, and F. In 1986, he completed a staff tour as a team member in the Headquarters USAFE Standardization and Evaluation Division. While on temporary duty at Taif, Saudi Arabia, he flew 34 combat missions in support of Desert Storm. He graduated from Air Command and Staff College in 1992 and from the School of Advanced Airpower [illegible] in 1993. Currently, he is serving as an action officer in the J-5 Directorate of European Command, Stuttgart, Germany.

Chapter 1

Introduction

Of what use is any ultra-advanced weapon, or superbly armed combat unit without a means of communications to bring it into play at the right time and with the right objective.

—Gordon Welchman
The Hut Six Story

It is easy to find quotations that emphasize the importance and decisiveness of command, control, communications, and intelligence (C^3I). Although not a panacea target, communications is a target to be attacked or exploited, regardless of the type conflict. Our libraries contain abundant data on C^3I and the structures supporting them. However, I challenge any reader to find information on how to target communications. There is simply little available, much less a single source document on the subject.[1] It is ironic that what allows a military to perform its mission is not seriously analyzed as a target set other than to categorically restate the obvious and say it is important and should be attacked.[2] Also ironic is the fact that "the relationship between [communications and] military effectiveness is neither widely understood nor widely appreciated."[3]

This thesis provides the campaign planner with an understanding of telecommunications and how best to attack them. I chose to examine telecommunications because it is the only form of communication that has the capacity to process the quantity of diverse information necessary to fight successfully against the US at the operational level of war. It permeates every face of society, thus allowing exploitation of information throughout the conflict spectrum at the tactical, operational, and strategic levels. Because of its data transfer capacity and its mobility, telecommunications continues to increase in importance as a medium to direct our national instruments of power. Conversely, we must strive to deny the enemy the use of their telecommunications.

A complete analysis would separate communications into its two subsets, supply and demand. Demand investigates "why" we should attack communications. It defines the impact of attacking the information which passes within and between a nation's political elites, economic sectors, social groups, and military forces. Analyzing demand reveals the effects that exploiting information has on the above mentioned organizations, and ultimately measures the enemy's ability to wage war. This cause and effect relationship should answer questions such as: what political effects on

government, psychological effects on population, or military effects on fielded forces occur from exploiting communication systems.

While understanding both supply and demand subsets is essential to fully exploit a communications system, this thesis will focus only on supply.[4] Supply determines "how" to attack communications. It defines the medium in which information flows and the associated supporting hardware and software necessary to transmit and communicate on that particular medium. Generally, attacks on communications conjure up visions of destruction of a system with conventional weapons. In fact, much more is involved. One must analyze the system to determine its vulnerability to an attacker wishing to collect, disrupt, delay, deny, or distort information through the use of either lethal or nonlethal methods. It is this physical medium which contains the clues and provides the opportunities for us to achieve desired effects.

I intend to provide a methodology which analyzes the telecommunications system and then describe both conventional and nonlethal kill mechanisms available to attack it. I will then establish guidelines to which the planner may refer when analyzing system vulnerabilities for the purpose of designing an attack plan against telecommunications. These guidelines will help select the appropriate weapon(s) to exploit each vulnerability.

Chapter 2 provides an overview of telecommunication systems, vulnerabilities, and targeting options. By understanding the design of a generic telecommunication system, one develops a capability to analyze any system. The chapter offers one method to analyze a system's vulnerabilities and suggests several measures of effectiveness to quantify degradation. Once vulnerabilities are identified, targeting becomes a function of marrying objectives to weapons technologies to achieve those objectives.

Chapter 3 will describe both conventional and nonlethal weapons technologies and their kill mechanisms. If one wants to fully exploit telecommunications, one must consider both lethal and nonlethal attacks. With an understanding of what nonlethal weapons actually are, their legal and technological roadblocks, and some of their advantages and disadvantages, the planner can better understand how to incorporate these mission-enhancing technologies into the guidelines presented in chapter 4.

Chapter 4 examines when a campaign planner should use nonlethal technologies. It also defines 14 factors one must consider when deciding between using lethal or nonlethal weapons to attack telecommunications. Some of these factors include the quantity, quality, and type of intelligence available about a network, and what type delivery vehicle is available. These issues are valuable not only to war fighters and campaign planners, but also to those responsible for writing doctrine, procuring C^3I systems, and developing force structure.

Inherent in all force structures is the communications necessary to control them. Many consider communications the "most vital of all combat commodities."[5] According to Soviet doctrine, loss of command and control at a critical moment has historically been one of the primary factors resulting in

defeat.[6] Therefore, we must first understand what a telecommunications system consists of and exploit its vulnerabilities.

Notes

1. The Air University Library has 926 references to either C^3I or telecommunications. None outline a systematic approach to targeting telecommunications. Some studies and reports address survivability issues such as vulnerability to EMP or lack of system redundancy, but none address the subject of targeting.

2. Col John A. Warden, *The Air Campaign: Planning for Combat* (Washington, D.C.: National Defense University Press, 1988), 56. In his book, Colonel Warden stated he found that "no really good examples exist of successful theater attacks on just the communications part of the command system." He reiterated this point in relation to Desert Storm in an interview I conducted with him in October 1992.

3. Paul B. Stares, *Command Performance: The Neglected Dimension of European Security* (Washington, D.C.: Brookings Institute, 1991), 18. A recent War College research report helps describe the relationship between communications and military power. The report describes COGs as elements of power which consist of three components: sources, linkages, and forces. Sources are singular substances which make up a society. They include elements such as technology, natural resources, social values, and the military. Force is the manifestation of these resources into instruments of power. Linkage is the conduit which metamorphizes the sources into force. Communications, therefore, is a link, not a center of gravity. While linkages possess no force in and of themselves, they "can possess either strength or vulnerability which can be exploited to disrupt a center of gravity." Lt Col Pat A. Pentland, "Center of Gravity Analysis and Chaos Theory" (Unpublished research report, Air War College, Air University, Maxwell AFB Ala., April 1993), 24.

4. Just as information on how to attack communications is sparse, so is that available for why to attack them. Page restrictions set on this thesis force deferment of a study of demand. However, the following describes what a full study of demand would entail: case studies should describe what effects can be achieved from exploiting communications between five categories. The categories include communications between governments, national political elites, political elites and the population, political elites and the military, military organizations, or a combination thereof. Each case should answer three questions. What were the desired effects, how were they achieved, and what were the results. The study would conclude with an analysis of how, and under what conditions, attacking communications within categories degrade enemy military capability.

5. Stares, 19.

6. Foreign Broadcast Information Service, *Soviet Union: Military Affairs, Tactics*, 29 June 1988, JPRS-UMA-88-008-L-1, 39.

Chapter 2

Telecommunications

Remove the communication links, and one is left with a collection of unconnected and therefore relatively useless items of equipment.

—M. A. Rice and A. J. Sammes
Communications and Information Systems for Battlefield Command and Control

This chapter describes what a modern communications system consists of (to include future trends), identifies its vulnerabilities, outlines various methods to attack it, and provides measures of effectiveness for postattack analysis. This in-depth analysis is important because as force size, spatial dispersion, force complexity, combat tempo, and the need for continuous twenty-four hour operations increase, electro-mechanical devices "become virtually indispensable to the collection, processing, and dissemination of information."[1] Late information, if only by seconds, can force an opponent into a reactive rather than proactive mode. Information dominance can act as a force equalizer for a weaker power, or enhance the capabilities of a stronger power. But, more importantly, it is critical when adversaries are closely matched, where just a slight differential of information between opponents may determine victory or defeat.[2] In order to achieve information dominance, the military relies on technology.

While technology is greatly expanding the sophistication and service level of telecommunications, it is also creating more vulnerabilities than ever before. To take advantage of these new vulnerabilities, intelligence organizations must collect information about a system's enabling software and provide feedback on the effects of attacks which leave no visible damage. It is obvious that absolute measurement of system degradation will be virtually impossible, but measurements of degradation "is too important to be ignored or classified as just another intangible factor, like morale."[3] A commander can at least estimate the impact of his efforts against the enemy if he knows how the overall communications system has been affected—especially at the operational level where coordination of forces occur.[4] In order to better understand the result targeting a system has on the overall network, one must first understand how that system functions.

The Modern Communications System

Many describe the telephone system as "the most complicated machine ever constructed by human beings . . . ."[5] It combines physics, natural resources, and ingenuity into an unbelievably complex discipline called telephony. It should be no surprise that the average subscriber knows little about how telephony works. This lack of knowledge is not so much due to the subscriber's ignorance as it is to the telephone company's strategy to simplify the use of its service. Unfortunately, this strategy also affects those responsible for campaign planning. The following explanation of the modern communications system, although simplified, provides the planner the knowledge he needs to attack telecommunications. The best way to approach this task is to start with how a telephone call is routed to its destination.

When telephones were first used, each subscriber had a direct line to another. However, as the number of subscribers increased, this method became costly and unmanageable. As figure 1 shows, for everyone to have direct contact with every other user would require an enormous amount of wiring and switching capability. This type of system architecture provides a high degree of redundancy and survivability against physical attack, but is cost prohibitive and impossible to manage for large networks.[6] For example, to connect the 600 million telephones of the world in this manner would require 180,000,000,000,000,000 interconnections.[7] To solve this dilemma, telecommunication companies began to route subscribers through switching stations.

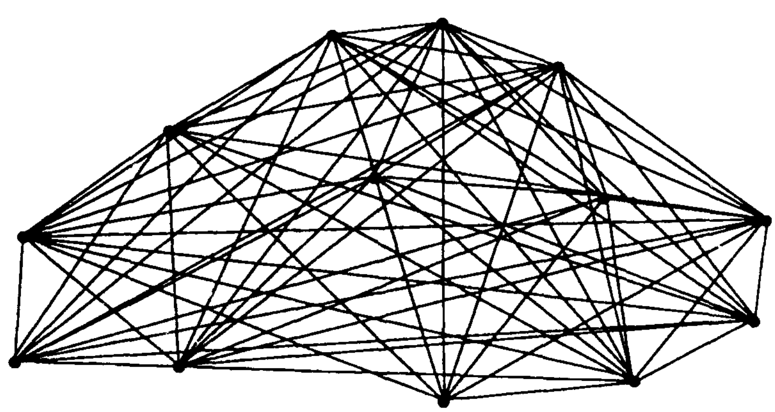


Figure 1

Figure 2 illustrates how all subscribers can be connected to a central switching station.[8] This approach is an improvement over the direct line system, but several problems still exist. First, destruction of one central node could render the entire system inoperative. Second, it requires a wire from each phone location to run the distance to the switching center. Third, the infrastructure necessary to connect 600 million wires converging from around the world would be unmanageable not to mention impossible to repair.

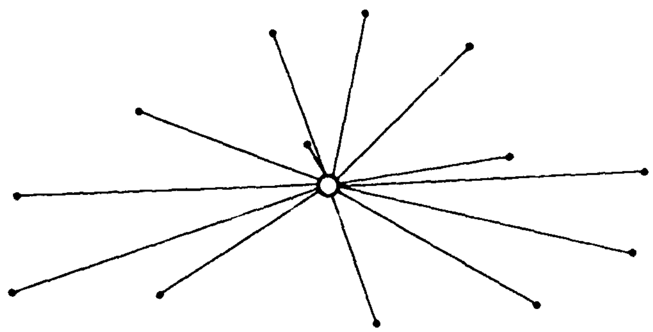


Figure 2

The most effective solution was a compromise between the two approaches. The solution incorporates both a series of switching facilities ranging from local, sector, regional, and international levels and amplifying stations to boost signal strength which attenuates between these switching facilities. With the exception of some future fiber-optic systems, long distance calls require numerous remote or manned repeater or amplifying stations. The medium determines the distance between these stations. A metallic landline may require one every five miles while a fiber-optic line may only require one every 40 miles. Generally, switching facilities are "the most critical elements in a telecommunications system. They are often highly automated, unmanned [or lightly manned], and remotely monitored."[9] They also house a certain percentage of the amplifying capability and the multiplexing equipment which will be discussed later.

The compromise thus works as follows: Connected to each subscriber phone box is a set of wires carrying the electricity, transmitting, and receiving capabilities necessary to communicate. The wires travel to a remote switching unit (RSU) which connects a small number of users in a local area (for example, telephone numbers assigned a 272-prefix). If a caller's destination is not within his RSU, his call is routed to a central office (or end office) where his call is transferred to any RSU within the central office's domain (usually within a city or perhaps a military base).[10] If the destination is outside the central office's domain, the central office will transfer the call to a toll office where the call will then be switched to another central office, an RSU and then to an individual phone or data receiving device. For short distances, a call could be routed from the first toll office directly to another central office. For longer distances, the toll office may transfer the call through a sector, regional, or international switch and then reverse the process until the call reaches another central office. Figure 3 shows one routing option a call may take from San Francisco to England.

Cellular phones work in a similar fashion. When a subscriber makes a call, he sends out a radio signal to a remote receiver located in various regions. The receiver closest to the transmitting phone picks up the conversation and relays it, usually by landline, to the nearest central office. From there it follows the normal routing described above. Naturally, cellular phones, just as all mediums except for fiber optics, transmit signals vulnerable to SIGINT collection.

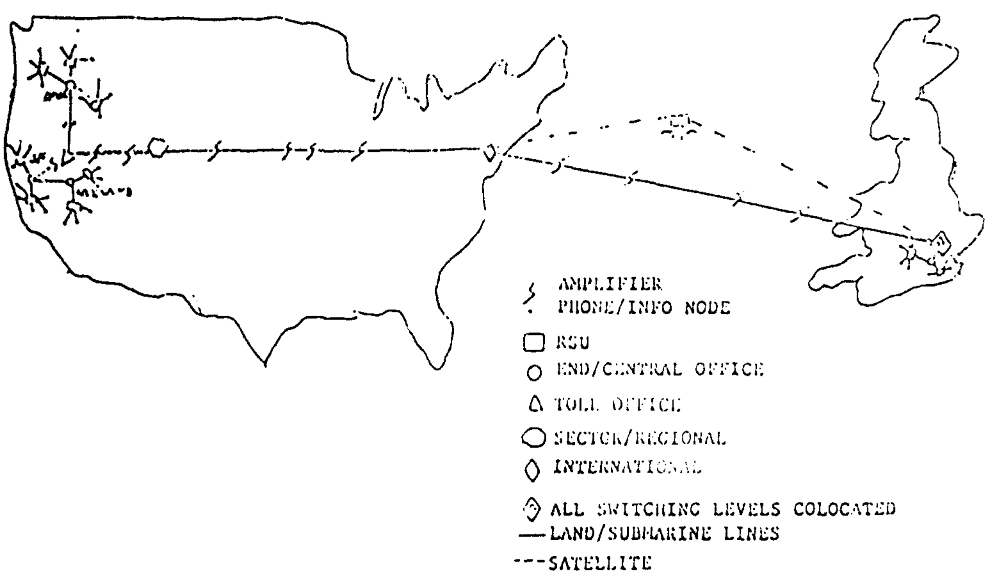


Figure 3

Figure 4 illustrates the complex maze of a switching hierarchy.[11] If one studies the connectivity in this figure, it becomes obvious how difficult it is to significantly degrade a system without a proper nodal analysis. There are an infinite number of ways a call can be routed when the preferred path is not available. With the advent of computerized switching technology, rerouting is almost instantaneous and is very effective at locating linkage between users. However, if access into the system is possible, a computer virus attack executed prior to, and in conjunction with, lethal attacks may provide a more uniform effect and a greater degree of total degradation. If a nodal analysis is not possible (as in a crisis situation requiring immediate action), virus attacks may be able to seek and then disrupt critical nodes not struck by conventional weapons. Beyond understanding communications nodes, one must also know how information is transmitted from one node to another.

A telecommunication system passes information over three types of mediums. They include landlines, satellites, and radio/microwave relays. Currently all but landlines are very susceptible to signal intelligence collection. Recent developments in each of these mediums provide vast communicating capability. For example, in 1983 one coaxial cable provided a maximum capacity of 10,500 voice channels. In 1988, one fiber-optic strand, ten times smaller in diameter than a human hair, could accommodate over 40,000 channels simultaneously.[12] The ability to achieve such tremendous communications capacity is a result of multiplexing—changing the frequency or alternating the timing of a signal transmission so that many signals can be transmitted on the same channel without interfering with each other. Without the ability to multiplex, even with extensive switching systems, "we would still require a large number of wires, one for each potential simultaneous conversation between two points."[13] Multiplexing normally

occurs at the switching office and is one of the most critical subcomponents of a telecommunications system. To continue the review of a telecommunications system, I now turn to the configuration of landlines, satellites, and radio/microwave relays.

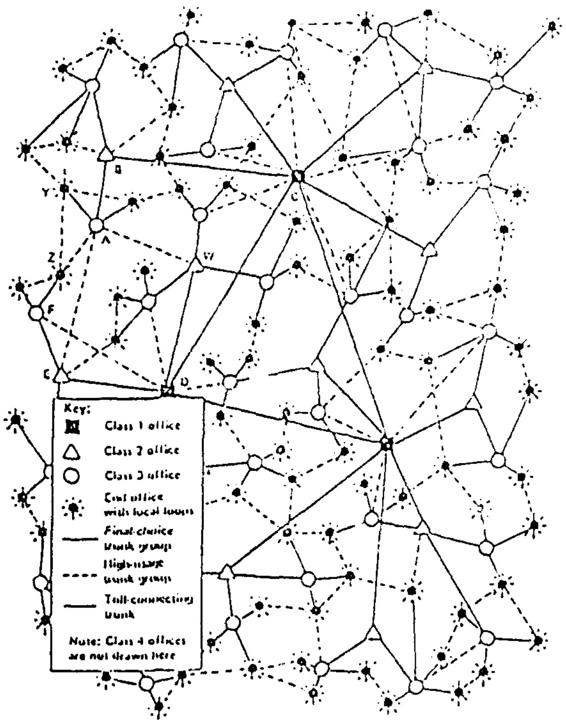


Figure 4

The diversity of mediums complicates the task of defining a system's architecture. The various mediums can be used in any combination between switching stations depending on a myriad of variables such as user's needs, terrain, security, and cost. Satellites and microwave/radio relays have the capability to bypass one or all switching stations. At one extreme, if a user is willing to pay the price, he can lease satellite channels and transmit and receive directly from desired locations, bypassing all stations or connecting to just the ones he specifies. The planner must also realize that adversaries have the ability to reconfigure their communications structure rapidly in response to destroyed nodes.[14] This is especially true at the tactical level. At the operational or strategic levels, repairs of main switching stations become much more difficult, and therefore depend more on redundancy than repairability.

The variables influencing the medium or combination of mediums in use also complicates target attack planning. Most phone calls within a country are normally routed via its civilian landline system because of the high channel capacity of fiber optics. However, a user may choose any medium he desires if he can afford it. For security reasons, someone like Saddam Hussein

may wish to have an unswitched direct line, microwave, or satellite link from his bunker to various military headquarters, even within a local calling area. Mobile satellite, radio, or microwave systems further complicate the planning process. To ensure a system of this complexity functions reliably, it must be resilient against attack.

The entire telecommunications system incorporates self-protection and security devices such as surge inhibitors and encryption algorithms, and all have backup power sources that continue to keep the system operating for indefinite time periods, even after destruction of the national power grid.[15] Designers also ensure survivability in additional ways. They build in redundancy by laying back-up cables, duplicating management and control functions, hardening critical switching nodes, and providing alternate communication systems at critical nodes. Apart from physical protection, these backup measures also enhance routing adaptability and provide excess capacity.[16] As witnessed in Dessert Storm, Iraqi command posts were buried 25 feet underground and many of the telephone and fiber-optic cables were also buried, making them very difficult to attack.[17] Not only do these initiatives increase survivability against attack, they also complicate an intelligence unit's ability to locate them and analyze system capabilities.

A lack of self-protection measures can jeopardize an entire operation. The primary maintenance and logistics network used in Desert Storm provides a good example of how US forces broke many of the rules of telecommunications survivability. Fortunately, we did not have to pay the consequences for these violations because the enemy was unable to attack Thumraite Oman located in the southern Arabian Peninsula. The US logistics system used in Desert Storm relied on a very fragile network dependent on two key nodes—one being centralized switching at Thumraite and the other being the satellite relay between Thumraite and the United States. A well placed bomb would have significantly disrupted the requisition and distribution of spare parts and other war material essential for maintaining high aircraft sortie rates. Figure 5 depicts how excessive centralization increases network vulnerability.[18]

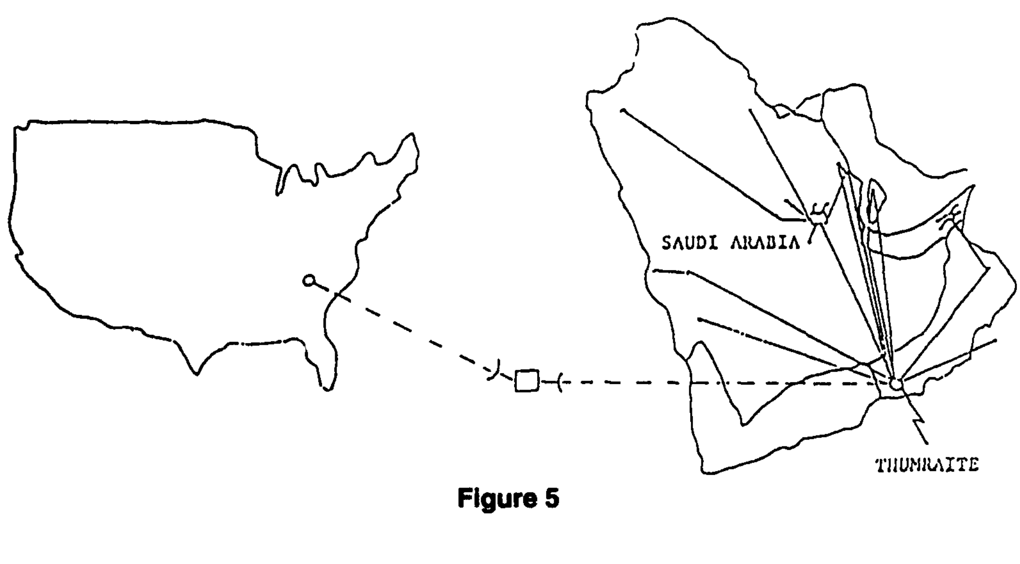


Figure 5

The Thumraite example, however, does not show the total vulnerability of modern information systems, which are increasingly dependent on computerization and satellites. The trend to simplify information management combined with the desire to save money helps ensure future telecommunication systems become even more dependent on computerization. This exposes communications software and electronic components to nonlethal technologies as though it were a crab stripped of its shell. Four trends in particular already verify these new vulnerabilities.

First, it is no longer necessary to depend on the slow mechanical switches used in analog systems. Computerization provides an exponential increase in capability through the use of digital technology. However, this increase in capability comes at the cost of network software vulnerabilities. Virtually every aspect of the telecommunications system depends on software—a vulnerability which future nonlethal technologies may easily exploit. Any nation wishing to compete on the modern battlefield must rely on digital communications software and hardware to achieve the data rates necessary to integrate complex war-fighting systems.

Computerization does enable one to disperse critical functions, but this entails higher costs due to the increased requirement for high-tech systems operators at different facilities. However, computerization also provides attractive cost savings through more efficient centralization. This is especially true of more sophisticated networks. Due to the complexity and expense of today's networks, management of the entire network becomes more critical and more difficult. Ability to oversee the entire network in order to monitor and repair network functions becomes very costly. Figure 6 illustrates the most cost-effective organization of the command and control function, and also the most vulnerable. If the regional management and control facilities cannot take over the central facility's duties after an attack, huge effects become possible from limited and insidious lethal and nonlethal attacks at lower levels. Any type attack then becomes more difficult to counteract. While centralization increases vulnerability to both lethal and nonlethal attacks, decentralization favors a nonlethal approach—a fact I will later demonstrate.

The second trend is that computerization may change the current organization of command and control:

> The rapid distribution of information and its effectiveness display will allow greater dispersion of the command and control function, which should increase their chances of survival. It will also allow a greater degree of flexibility in the

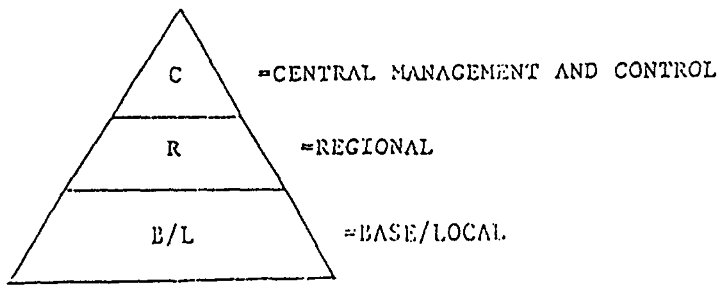


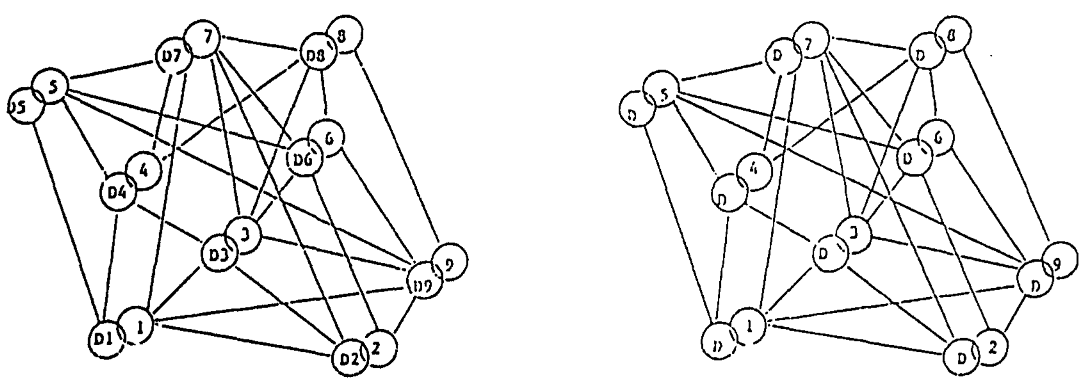
Figure 6

composition of headquarters, so that they may be more responsive to changes in tasking.[19]

A recent paper distributed by the Office of the Secretary of Defense concluded that failures in "realizing the great increase in military effectiveness was not so much a case of the political and military leadership of a state ignoring technological change, as it was a failure to see and initiate new operational concepts and organizational innovation."[20] The present military command system is centralized and vertical. As computerization provides the ability to maintain global data bases, command can become decentralized and horizontal. As each headquarters acquires the ability to maintain similar data bases, redundancy of command and control increases and coordination requirements decrease. "Modern telecommunications and microcomputer technologies make possible distributed information processing which reduces dependence on a centralized capability."[21]

One of the main benefits of decentralization appears in the composite wing concept. All headquarters has to do is give one order to the wing such as degrade X airfield by Y percent for Z days. Theoretically, the wing would have all the information available to achieve mission-type orders rather than depend on a centralized headquarters to produce an Air Tasking Order, as in previous conflicts. A command structure such as this reduces mission complexity by saving time and minimizing coordination requirements. Figure 7 illustrates the current as well as future command structures.[22] Note in the figure on the right, each of the nine nodes maintains the global data base represented by "D". However, while the redundancy of a global data base decreases vulnerabilities from conventional attack, it alternatively subjects the entire global data base to nonlethal attacks. As more information is shared, connectivity between all nodes increases, thus providing an opportunity to exploit or degrade the entire system in a short period of time.

The third trend is that modern militaries are becoming increasingly mobile and more dependent on information to operate their high-tech equipment. During Desert Storm, virtually every soldier had access to a GPS receiver. Satellite communications are becoming almost personalized, limited only by



EACH HQ ONLY HAS ITS OWN DATA BASE

EACH HQ HAS THE GLOBAL DATA BASE

Figure 7

channel availability. As this trend continues, nonlethal technologies capable of exploiting satellites will become a valuable addition to anyone's arsenal. A current USAF initiative called "Reach Back" serves to illustrate future dependency on satellite systems. The purpose of Reach Back is to provide all the computing capability necessary to support a rapidly deployed Air Force without forward deploying the hardware. The intention is to maintain computers and data bases in one or two Stateside locations to perform computations. Then each deployed unit requiring access to the data base will "Reach Back" to the States via satellite communications.[23]

This program illustrates the trend towards dependency on satellite communications. Ironically, as the US military ties itself to the satellite tether, it also recognizes the inherent vulnerabilities of space assets. After the Gulf War, a DOD report to congress acknowledged that "most SATCOM was vulnerable to jamming, intercept, monitoring, and spoofing, had the enemy been able or chosen to do so."[24] Additionally, policymakers are starting to take space campaigning more seriously. The new draft of the Air Force's space operations doctrine manual states:

> The space campaign will employ air, ground, naval, and space assets to delay, disrupt, deny or destroy threatening space systems, including up and down links; and TT&C nodes. These targets will be coordinated with all elements of the joint campaign plan to ensure space superiority. In many cases, the space campaign will precede air, land and naval campaigns since it makes our adversary 'deaf and blind' to other terrestrial operations. No precedents have yet been set concerning attacking an adversary's space capabilities . . . .[25]

Fourth, there is a significant trend towards the military depending on civilian systems for a greater percentage of their overall capability.[26] This is due mostly to cost, and as perceived threats dissipate, the Congress is less likely to fund separate military communications projects such as MILSTAR. The US is not the only country faced with this potential problem.

Even totalitarian countries depend heavily on civil systems. During the Gulf War, 40 percent of the total Iraqi civil system was dedicated to military use.[27] During the same war, the US depended on civil systems for 24 percent of its satellite communications in and out of the Kuwaiti Theater of Operations.[28] The move towards shared civil and military systems also increases potential vulnerabilities. Civil systems typically are less hardened and currently contain fewer encryption and self-protection capabilities than military systems. Whichever direction technologies take the development of communication systems, the potential for exploiting vulnerabilities will most likely increase.

Vulnerability Analysis

The complexity of modern communication systems necessitates a thorough analysis to effectively attack it. This analysis requires a great deal of intelligence collection, therefore, it is critical to gather information on an

enemy's communication systems well before hostilities. This will provide the time necessary to apply that information to an attack methodology.

The method this thesis uses is a modified open systems interconnection (OSI) framework. I chose this for two reasons. First, it separates a computerized telecommunications system into its component parts in order to isolate and identify vulnerabilities as they apply across the spectrum of the system's enabling software and hardware. Because of network computerization, exploiting telecommunications through its software will provide a valuable targeting option for the future. Besides transmissions, a telephone network must also transmit instruction operating.[29] The OSI layers are where these instructions reside. The second reason for selecting the open systems interconnection methodology is that the International Standards Organization (ISO) recognizes the OSI architecture as the world's standard for development of future telecommunication systems.

The OSI infrastructure currently consists of seven layers, each providing a specific service within the total system. As technologies improve, or additional services are desired, layers can be added to accommodate. The various layers and their functions follow.[30]

1. Physical layer—the underlying information exchange medium and modulation technique. This layer deals mainly with voltage requirements, uni- or bi-directional capabilities, number of pins per connector, and purpose for each pin.

2. Data link layer—the software/hardware that ensures access and acceptable error rate transmission of data bits across a single link in the network. This layer regulates the flow of information bits. In doing so, it ensures the number of bits transmitted are also received.

3. Network layer—the algorithms resident in the network nodes which provide transport of data packets (a single unit of information, including data and control elements, that is passed between adjacent nodes) across the network, from originator to destination.[31] This layer knows the topology of the system thereby chooses the most efficient routing of information to its destination. In doing so, it also controls congestion and connects multiple networks (internetworking).

4. Transport layer—the algorithms responsible for establishment, maintenance, and detection of connections between users of the network. This layer in essence provides quality improvements in the network layer and enables error free transmissions between two different type systems.

5. Session layer—the algorithms which establish, maintain, and disconnect the user from the network. It also keeps track of whose turn it is to speak and provides synchronization to correct noncommunication type errors.

6. Presentation layer—the algorithms related to information syntax (the resolution of syntax differences between users). This layer especially concerns itself with providing compatibility between various computer languages. It is also the easiest layer to induce encryption.

7. Application layer—the algorithms specific to the system being served, dealing with the semantic content of the information. It provides information to the user in a recognizable form, such as voice, E-Mail, text, etc.

Ability to access the application level in order to manipulate information is the most difficult because it requires knowledge of all previous layers. Since the application layer contains the actual information the user receives, it is an ideal target for a misinformation campaign. By injecting false traffic into a system, an attacker can "dilute or destroy mission effectiveness."[32] These types of attacks were successful in misvectoring attack aircraft during the Vietnam conflict.[33] Ability to issue false orders or situation updates could be more serious. Fortitude, the allied code name for the deception plan associated with Operation Overlord, documents the detrimental effects of false information can have on an enemy's ability to fight.[34] The other six OSI layers control system functions. In other words, they specify the system protocols (rules which define how information is exchanged throughout the network).

Falsifying information sent to the application layer can be diabolical and rewarding, while disruption of any of the other six layers can be fatal to the network. For example, if an enemy is able to gain access to the "network layer," he would be able to misroute information throughout the entire system. This tactic could serve several purposes. First, because the intended user never receives the information needed, it is as though the system was inoperable. Second, because numerous network subscribers will receive superfluous information, they waste time sorting out what they received and potentially enter a state of confusion as to what to do with the information. Third, continuous routing commands could lock up the system resulting in busy tones for all users or a crash of the entire system. The synergy of these type effects can devastate command and control.

To complete the system analysis, three additional categories which address the actual physical properties of the system are added to the OSI layers. While the OSI layers define how the system operates and what services it provides, these additional categories define the physical properties of the system.[35] Together, the OSI layers and these three categories, provide the analyst the information he needs to decide whether to use lethal or nonlethal attacks on the system. The three categories include—

1. network topology—physical layout of network nodes and links;
2. physical placement of assets—location of all equipment and facilities in the network; and,
3. choice of equipment—digital verses analog, landline verses other mediums, etc.

It is necessary to examine these three perspectives for they help identify system vulnerabilities to physical attack.[36] For example, "the placement of assets and back-up assets all within a single small vicinity could result in a physical attack removing all capability at a node."[37]

We can now visualize where the system's vulnerabilities may reside in each layer or category by comparing them to five perspectives common to telecommunication networks. The perspectives include—

1. network configuration—physical properties of a network;

2. access—susceptibility to enemy access into the system;

3. protocols—once access is gained, how susceptible are the system's data transfer service, routing, flow control, etc.;

4. management and control—information concerning network ability to adapt to congestion, adaptive routing, etc.; and,

5. information—mission related information actually received by a user/decision maker.[38]

Figure 8 graphically depicts this complex relationship. For example, six of the OSI layers have protocols associated with them which may be vulnerable. It

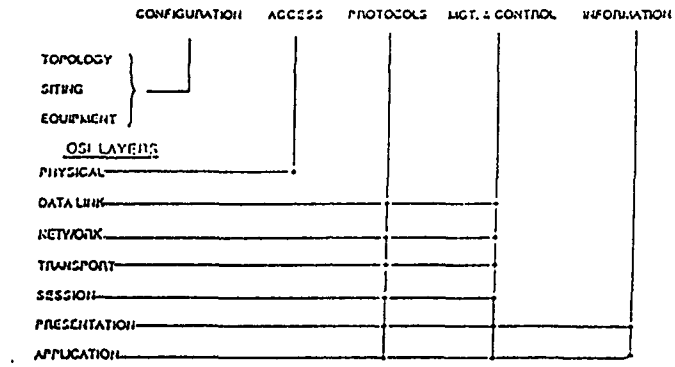


Figure 8

also shows that to affect the information perspective, one would have to successfully penetrate either the presentation or application layer.

To complete the vulnerability analysis, figure 9 indicates the analyst must ask four questions about each perspective to determine its vulnerabilities.[39] First, how *susceptible* is a system architecture to interference. Second, to what extent can one *intercept* network information flow describing how the system works thereby gain the knowledge necessary to disrupt the network. Third, is it possible to gain *access* to the network to interfere with its functions. Fourth, is it *feasible* to attack the system (e.g., do the objectives of attacking or

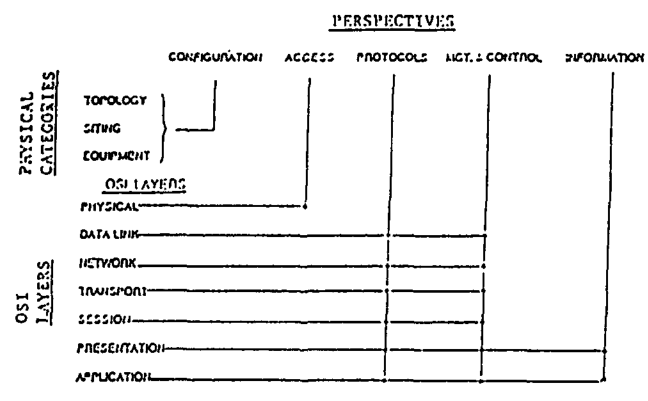


Figure 9

penetrating the system, or parts of it, justify dedicating the resources required to obtain those objectives).

The answer to each of these questions must be "yes" in order for a layer or category to be vulnerable to attack. In other words, if a layer is susceptible to an attack, but access cannot be gained, then that layer is theoretically not vulnerable. For example, to analyze the "network layer's" protocols, one would ask if they were susceptible, interceptible, accessible, and feasible to attack. The same four questions would be asked of each perspective. The following provides an example of what type question an analyst would ask relative to each perspective (see appendix A for a complete list of questions).[40]

1. Configuration—Are there critical nodes the loss of which would inordinately degrade network performance?

2. Access—Can an adversary with adequate communications resources enter the network as though he were a friendly network node?

3. Protocols—Can protocol parameters be altered resulting in network performance degradation?

4. Management and control—Can an adversary induce deadlock by exhausting message buffer space at a node?

5. Information— can fictitious or corrupted user data be delivered over the network by a spoofer who has joined the network?

The above analysis, however, only addresses the systems owned by an adversary.

There are some vulnerabilities which may require the cooperation of another nation in order to deny information to an adversary. For example, the satellite providing information to an enemy may belong to a neutral third party. This in fact occurs routinely in both civilian and military information systems. Russia openly advertises its satellite intelligence capabilities for the right price.[41] These information sanctuaries were of a major concern to Coalition forces during Desert Storm and will present a greater problem in the future as information systems become more internationally dependent.

At another extreme, the attacker himself may depend on the same satellite for the same information he wishes to deny to his enemy. Even US forces depended on other nations for information support during the Gulf War. Besides acquiring additional communications capabilities from Coalition systems, the French SPOT satellite was critical in remapping Iraq and Kuwait. It should now be apparent that communication systems can be vulnerable in numerous ways. Once the campaign planner identifies these vulnerabilities, it is then time for him to target them.

Targeting

When exploiting a telecommunications system, the campaign planner must choose one of three attack methods—physical, jamming, or spoofing. Figure 10 relates the OSI vulnerability analysis from the previous section to these type attacks. The figure shows that each perspective should be reviewed for vulnerabilities to each type attack.[42] For example, after completing the

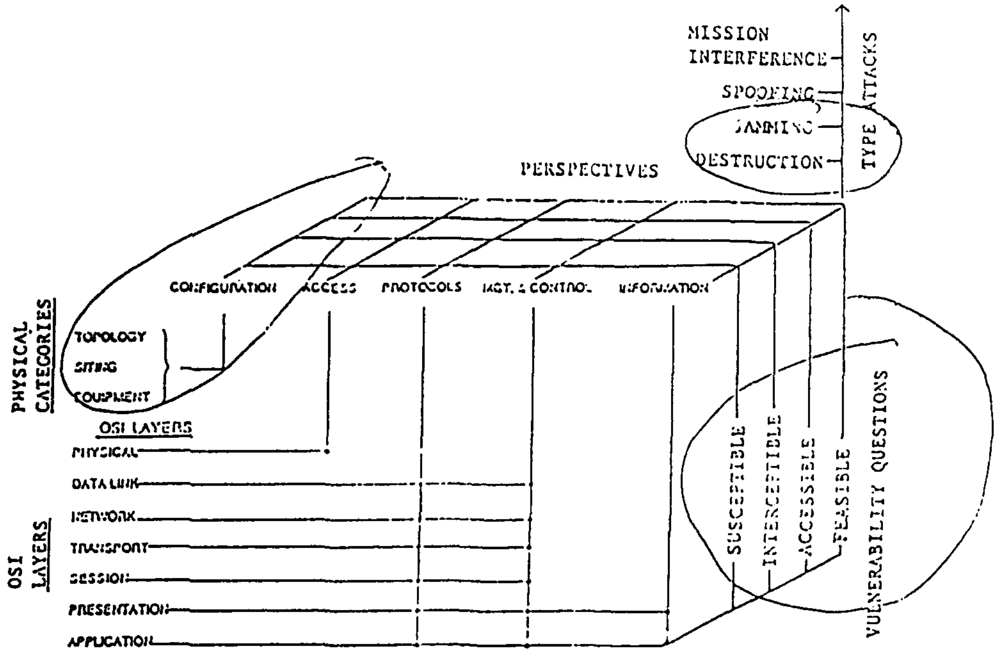


Figure 10

vulnerability analysis as explained in figure 9, one would then proceed up the vertical scale to determine best/alternative attack mechanisms. As one climbs the scale, the more sophisticated the information necessary to attack becomes.

Physical attack of the configuration is achieved by either conventional, nuclear, or nonlethal weapons (destructive nonlethal attacks may include EMP, high voltage surge weapons, etc.). The main consideration in physical attack is "the extent of damage which can be done to remote portions of the network from a localized attack."[43] System redundancy, centralization of key nodes, and hardness and location of those nodes will determine the resources required to obtain the desired system degradation from physical attack. Dispersal, hardening of key facilities, and rules of engagement all act to limit the effectiveness of conventional attack. For example:

> The fiber-optic network Saddam Hussein used to communicate with his field commanders also included many switching stations (one of which was at the basement of the Ar-Rashid Hotel) and dozens of relay sites along the oil pipeline from Baghdad through Al-Basrah to the south of Iraq. However, hitting some of these targets was not desirable despite their military significance, because of possible collateral damage.

Deciding to use physical force does not relinquish the requirements for detailed intelligence. If a system is quite sophisticated, it is important to know the location of key nodes and their backups. Even if the attacker has the necessary intelligence, he must be willing and able to expend the effort to attack the system, at the expense of other potential targets. A halfhearted attempt may do little to degrade combat operations. If the attacker

has (and is willing to expend) enough ordinance, he can destroy all of the network communications assets (provided he can find and target them, and render the communications network inoperable). Short of this extreme, however, there are two key questions which the topological susceptibility assessment must address relative to the threat of physical attack.

1. Are there any nodes that control the entire network. One must also look beyond the immediate network to see if there is a key node providing vital information to another network such as a weapon system.

2. Is it possible to locate and prioritize these key nodes to ensure maximum results from each bomb dropped.[44]

If the answer to these questions are uncertain or physical attack is not desirable, jamming or spoofing provide alternative attack options.

Jamming "focuses resources on particular links, messages, or time periods in order to have increased effectiveness in disrupting the network as a whole."[45] For example, jamming of satellite downlink receptions may effect an isolated area of the battlefield, but jamming uplink reception at the satellite will uniformly effect the entire theater.[46] If uplink jamming is not possible, jamming will be most effective when selecting a particular time and location to jam in order to achieve a specific objective. While jamming is usually understood to be the use of electronic interference projected at an electronic instrument such as a radio or radar dish, it can also be internal to the system effecting each of the OSI levels by introducing failure mechanisms such as harmonic disturbances. For a more sophisticated and uniform effect, an attacker can turn to spoofing.

Spoofing allows for "actual participation in the network by a sophisticated adversary, so as to disrupt communications by injecting false information into network control algorithms and protocols."[47] Spoofing can either attack one of the OSI layers, or the software within a system dependent digital information. It can create significant defects in a system, some serious enough to collapse the entire system. If the attacker has an in-depth understanding of and access to the system, "full participation in the network activity" is possible.[48] "With the ability to participate, he can accomplish such evils as withholding information, loading the network, [controlling satellite functions], or simply monitoring and controlling network traffic."[49] Monitoring network traffic has the additional benefit of identifying the location of key enemy C^3I nodes. One example of spoofing is infecting a network with a virus or a worm such as that which attacked the INTERNET system in 1988.

The INTERNET is an international network of 60,000 subscribers who share information for the purpose of research. The system consists of over one million host computers and at least 13 million E-Mail accounts. Although the virus did not attack network protocols, it did attempt to disrupt services and overload systems to cause lockup. And, while the virus did not spread outside of the INTERNET system, there were gateways to other networks. The military network (MILNET) and Defense Advanced Research Project Agency (DARPA) both shut down their access to INTERNET prior to being infected.

Others not so lucky, such as MIT's Lincoln Laboratories were brought "to their knees" within twenty-four hours.[50]

The virus spread via three different attack profiles so that if users discovered one, the other two could continue their mission. One profile had a very insidious side effect. It used the E-Mail service to enter the system. When discovered, the initial response to kill the virus was to cut off mail service, but this in fact allowed the virus to spread more rapidly because instructions could not be sent to users on how to destroy the virus. This allowed the other two attack profiles to continue throughout the system. The only fix was to shut down all computers until a team of America's brightest computer minds isolated and destroyed the virus.

There are some valuable lessons from this incident. First, this virus was somewhat clumsy and unsophisticated but still took two days for some of the world's best computer analysts to recognize, then another two days to fix. Regardless of how well-specified or reliable a system may be, software failures "can be extremely difficult to diagnose. . . ."[51] It is relatively easy to identify and repair an isolated node after physical damage. However, "when a software-based system is modified, the effect of the modification on the whole system must be considered," and even then, comprehending all possible effects may not be possible.[52]

The friction of war makes the situation even more detrimental. In the midst of combat, identifying that a subtle software problem exists, then actually locating someone capable of repairing the malfunction could be a real challenge. This would especially affect a third world country not having technically skilled indigenous personnel.

Repairs requiring system shutdown would further complicate enemy military operations rendering the system *de facto* inoperative and temporarily accomplish the same objective as if 100 percent of the system was physically destroyed. Additionally, the effort spent trying to work with an unreliable system can create even more confusion. It is unlikely most militaries have the procedures to cope with an attack of this sophistication, and if they do, it is doubtful they have validated them through exercises. This is because exercises are costly and by practicing degraded communications procedures, commanders sacrifice combat operational training.[53] A degraded system dependent on inadequate reconstitution procedures would severely effect a commander's capability to function.

Attacks become very insidious when one mixes lethal and nonlethal attacks. The synergistic effect of mixing lethal attacks and jamming (a form of nonlethal technology) have been well documented in attacks against air defense systems during the 1981 Israeli attack on the Bekaa Valley and the Coalition attack on Iraq. An ability to employ nonlethal attacks could make lethal attacks even more effective and efficient—if not unnecessary in some circumstances. One example of employing both type weapons would be to initiate an attack with nonlethal technology in order to disrupt communications and associated functions dependent on the system attacked (such as an air defense system). Then, after verifying the desired degree of degradation, a

lethal attack could commence. In any case, lethal attacks should accompany nonlethal attacks in order to mask a main attack on the OSI layers. By doing so, repairs are focused on the physical damage thereby delaying repairs to the real problem. This leads to further confusion and immanently, command paralysis.

It is possible for the command and control to enter an infinitely increasing destructive loop as shown in figure 11 (the trinity of communications targeting). As chaos theory predicts "small changes in the definition of a system design may result in a very large and unpredictable change in the system vulnerability."[54] In addition, changes in the network may transform initial susceptibilities into other types.[55] As this occurs we penetrate an adversary's command and control loop and ultimately his ability to comprehend or react to problems. One author calls this getting inside the adversary's "O-O-D-A Loop" which is his "observation-orientation-decision-action" process.[56] If one is able to operate just ahead of an opponent's O-O-D-A Loop, he can void the enemy's strategy. The opponent becomes reactionary and unable to coordinate coherent operations.

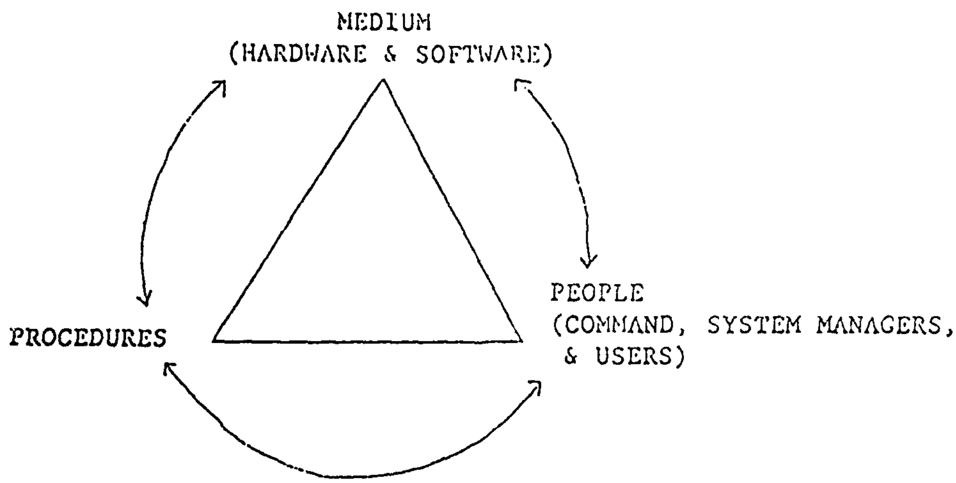


Figure 11

At this point, I would like to reemphasize that the information necessary to spoof a system is complex, requiring a well developed intelligence portfolio long before a conflict begins. An understanding of the system's authentication procedures, access control, data confidentiality, and data integrity is necessary to fully participate, especially at the application level.[57] However, once a system is infiltrated, the potential damage may far exceed that possible by physical attack. An entire system can now be effected and provide little to no indication of damage until it is to late to react. The following warning serves to illustrate the inherent vulnerability of future communication systems.

> The more complex the automated system becomes, and the more the users come to depend on it, the more difficult will it be for them to do without it. It also goes without saying that any fallback mode, whether partially automated or fully manual will represent a considerable reduction in capacity.[58]

Ability to measure this reduction is an essential element of the targeting process, therefore it is discussed in the following section.

Quantification

Quantification of network degradation is necessary if the commander is to make an intelligent estimate of a resultant degradation in combat effectiveness. To begin, one must first determine what percent of a particular system an adversary needs to effectively operate. For example, even at peak usage rates, a military may require only a small percent of the civil system it is sharing. This being the case, it becomes apparent massive damage is necessary to degrade a system to this level. In addition, as degradation occurs, the government can begin controlling access to the system and prioritize calls in order of military importance. It is true that while the system is operating at a reduced level, little additional degradation is needed to effect military capability. On the other hand, operating at this reduced rate also reduces the quantity of repairs required.

The quantity of information a military needs depends on many variables. The US intelligence agencies, integrating an enormous amount of information from many sources, would require a much larger communications capacity than most any other national intelligence agency. The same can be said for functions such as logistics support and operational control—especially for deployed forces. This demand analysis can be applied to all military functions taking into account variables such as size and complexity of forces, command and control philosophies, and tempo of battle. If these communication requirements are known, the analyst can use the following measures of effectiveness (MOE) to help assess system performance before and after attack.

The first MOE is grade of service (GOS) which determines the loss of system capability in a static (nonmobile) system. To determine GOS, divide the traffic available after attack by the traffic offered by the original system capability. However, for GOS to be a valid indicator of combat effectiveness, it is necessary to know what percent of system capability is actually needed for military operations. All systems have a certain amount of slack and can provide some surge capacity. Therefore, a 30 percent reduction in system capability may not significantly effect military communications. Rerouting, prioritization of transmitted information, and cutting off civilian use could nullify even a large reduction in system capability. Also, to make a valid assessment of degradation in combat effectiveness, knowledge of what level of leadership an attack will effect is necessary. Although situation dependent, in most cases degradation at the operation level would effect an enemy's ability to coordinate forces and ultimately his combat capability the most.

The second MOE is the range that information can be heard. For example, jamming may overpower a radio's ability to receive if beyond 1000 feet. While

at the OSI levels, jamming of information may attack the quality of information before it is picked up by the receiver.[59]

The third measure of merit is throughput and delay. Throughput is the "amount of successful data transmissions over a unit of time."[60] Delay is the time between data transmission and reception. These two parameters are the most used MOEs in civil systems to measure performance. The relationship between these two are that if throughput increases, then so does delay and vice versa. One becomes keenly aware of this relationship when trying to place a call on Mother's Day. These MOEs are susceptible to attack on both the topology and OSI layers. By decreasing nodes through destruction, other nodes compensate by taking on a greater load, thereby reducing throughput and creating information delay. Attack on the OSI levels can overload throughput or intentionally create delays in the system by manipulating network protocols or transmitting excessive information packets.

The fourth MOE is utilization which defines how much surge capability is available. This is the difference between normal usage and peak-capable usage.[61] Knowledge of this measure of merit gives the planner an idea of system degradation necessary before an enemy is forced to compensate for additional damage to his system.

The fifth and final MOE is availability. In effect, this is the goal of attacking communication systems, for the system must be available and functioning to have merit. Two categories under this MOE are reliability and survivability.[62] Reliability is the capability of a system to provide information to the user. For example, if the system becomes congested causing rejection of a percentage of the information, it becomes unreliable.[63]

Survivability is the network's ability to continue to operate after attack from either physical damage, jamming, or spoofing. After physical attack, a measure of survivability is the "percent users still communicating versus the number of node sites destroyed."[64] This is one area battle damage assessment (BDA) is typically misrepresented. Normally, an analysis would look at 50 percent of the nodes destroyed and equate that to a 50 percent degradation in system capability. In reality, however, this relationship is nonlinear and is a function of demand on the system and how it compensates for degradation. Up to a certain amount of damage a system will experience little depreciation in system performance. However, past that point any additional damage will most likely cause a disproportionately larger degradation in combat effectiveness, unless demand is controlled or reduced (see fig.12).[65]

Battle damage assessment must be sensitive to total system effects, not just percent damage. This will be a difficult challenge when analyzing effects of attacks on the OSI levels, but it is important the intelligence community start thinking in this paradigm. Desert Storm has already demonstrated that conventional BDA methods are inadequate for smart, penetrating weapons, they are even less adequate for nonlethal attacks.

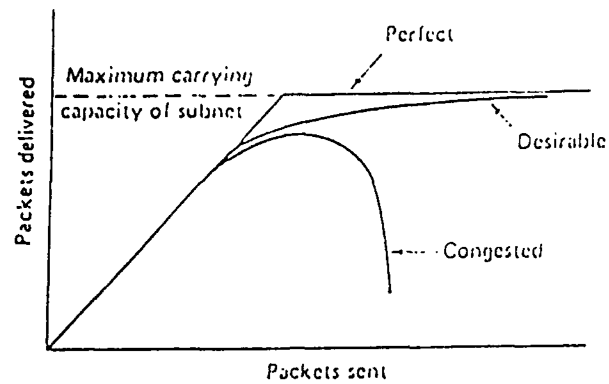


Figure 12

Conclusion

The targeting of communication systems must emanate from an understanding of how communication and information systems work, the capability of the particular system targeted, and how the enemy plans to use that system. Without this knowledge, the targeter has little hope in designing a successful campaign against an adversary's information network.

This chapter presented a methodology to aid in the procurement of this knowledge. This method analyzes both the topology and OSI layers to identify system vulnerabilities to either lethal or nonlethal attacks. It guides targeters, vendors, contractors, HUMINT sources, academia and government agencies to answer questions such as: is the system centralized, do the number of nodes make physical attack impracticable, what are the backups, are there key nodes not accessible by conventional weapons, and what vulnerabilities do the system OSI layers present.

I also describe five primary targets within a telecommunications system. They were switching centers, management and control facilities, multiplexing facilities, transmission mediums, and repeaters or amplifiers. Some nodes house all the above transmission components making that particular node critical, hence a high priority target. For uniform effects, I recommend attacking these critical nodes at the most centrally controlled level as possible. For a more local effect, one should target similar facilities at the central office or lower. In each case, deciding on which component to take out, and whether or not to use lethal or nonlethal weapons, is a responsibility of the planner. He should base his decision on information such as mission objectives, desired effects, attack assets, weapons capabilities, available intelligence, ROE (constraints and restraints), and the ability to assess battle damage.

The potential reward for pursuing the ability to attack communication and information systems with nonlethal technologies is worthwhile. However, to shift to this paradigm will require a revamping of intelligence gathering and damage assessment techniques. In the past, battle damage assessment of

system topology after lethal attacks was fairly simple. However, ability to determine overall system degradation was very limited. Battle damage assessment of nonlethal attacks is even more difficult to quantify, but if this capability is achieved, the ability to assess lethal attacks will also improve.

To coordinate pre and poststrike analysis, there needs to be an organization designated to collect information on national telecommunication systems from a holistic approach well before a conflict begins. The organization needs to incorporate lethal and nonlethal attack options and viable BDA procedures for each option. Some measures of effectiveness BDA should answer are grade of service, range of information, throughput and delay, utilization and reliability. In addition, a cadre of personnel able to speak the language and understand the culture of the enemy will benefit the BDA process. The organization also needs to know where to find information on certain countries and if necessary maintain HUMINT within the country to track new system developments and anomalies or to gain physical presence to enable access to closed systems. The goals of the organization would be to know all communications capability within the country, determine what percent of the system the military requires to operate effectively, make recommendations about attack options (physical attack, jam, or spoof), and quantify system degradation after attack. To accomplish this latter objective requires a close intelligence/operations relationship. The more the intelligence support knows about the overall objective, the better able they are to assist. Accomplishment of these goals are necessary requisites to estimating degradation of enemy combat effectiveness.

Based on the scenario and enemy capability, the targeter has two targeting options—lethal or nonlethal. In both cases, attacking key nodes, such as central communications management and control centers and critical switching/multiplexing stations, will achieve the most effect for a given effort. Lethal attacks may limit effects to areas attacked if enough assets are not available or rules of engagement prohibit casualties or collateral damage. Nonlethal attacks may expose a larger percentage of the system to degradation while keeping the infrastructure in place for postwar recovery. Regardless of the type attack selected, effectiveness of the attack and political ramifications of the methods used are essential to determine how to attack the system.

Because of the ability to more fully exploit a network, this study concludes that the ability to attack computerized telecommunications at the OSI levels would make a valuable contribution to information warfare. Simultaneous lethal and nonlethal attacks on a network would result in a synergy, magnifying the effects of the attack.[66] To delay research towards the ability to execute nonlethal type attacks will stagnate the US in the old paradigm of the American way of war—physically destroy everything to ensure success. Over 60 years ago, Guilio Douhet presented a similar warning. In his book *The Command of the Air*, he said "victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adopt themselves after a change occurs."[67] The ability to manipulate digital information is not a

problem of the future, but one of the present. Computer hackers, some using unsophisticated methods, "can potentially shut down our high-tech society."[68] Based on US military strength, it is feasible nonlethal attacks on information systems will be an adversary's only effective capability to cripple the US. Therefore, I recommend research and development of nonlethal attack technologies for telecommunications if for no other reason than to learn how to protect our own system from these type enemy attacks. The next chapter explores the characteristics of both lethal and nonlethal weapons technologies that offer this expanded attack capability.

Notes

1. Paul B. Stares, *Command Performance: The Neglected Dimension of European Security* (Washington, D.C.: Brookings Institution, 1991), 48–49.
2. Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics 1851–1945* (New York: Oxford University Press, 1991), 8.
3. Stares, 45. The number of ways an opponent may compensate for system degradation are infinite and limited only by the imagination. For example, during Desert Storm, the Coalition communications architecture was designed from scratch with modifications made as needs evolved. Also, one cannot underestimate the value of the courier. Although this method is not effective for rapidly changing conditions, it does serve a useful purpose. Highly classified information can be sent this way to prevent interception or, as the US did in the Gulf War, large volume information packets sent by courier can free overcrowded telecommunications lines. The courier system was the method the US adopted to send the daily Air Tasking Orders to each of its bases. It was the only way to get the information to the Navy's carriers.
4. Stares, 152 and 167.
5. John R. Pierce and A. Michael Noll, *Signals: The Science of Telecommunications* (New York: Scientific American Library, 1990), 4.
6. David J. Morris, *Communication, Command, and Control Systems* (New York: Pergamon Press, 1977), 115; and James Martin, *Telecommunications and the Computer* (Englewood Cliffs, N.J.: Prentice Hall, 1990), 443.
7. Martin, 441.
8. Morris, 115; and Martin, 443.
9. DCSINT, USA Special Operations Command, *Special Operations Targeting Handbook*, October 1991, 101.
10. Often times, a military base will have at least one central office making an excellent target if isolated effects are desired. However, one must also consider the possibility of additional civilian capability such as pay phones or other devices leased by the government from a civilian company. These systems do not normally route through the base switching office.
11. Martin, 444.
12. Pierce and Noll, 132.
13. Herbert S. Dordick, *Understanding Modern Telecommunications* (New York: McGraw Hill Book Co.,1986), 47.
14. Foreign Broadcast Information Service, *Soviet Union: Militry Affairs, Tactics*, 29 June 1988, JPRS-UMA-88-008-L-1, 48.
15. Dawn Bushaus, "Hugo No Match for So. Bell," *Telephony*, 25 September 1989, 3.
16. Rome Air Development Center, *Network Vulnerabilities Study*, Final Technical Report RADC-TR-89-341 (Griffiss AFB, N.Y.: Air Force Systems Command, 1990).
17. Department of Defense, *Conduct of the Persian Gulf War*, Final Report to Congress (Washington, D.C.: Government Printing Office, 1992), 73.
18. Interview with Captain Burch and Master Sergeant Raphael, Standard Systems Division (SSC), USAF Communications Command, Maxwell AFB, Alabama, Gunter Annex, 26 February 1993.

19. M. A. Rice and A. J. Sammes, *Communications and Information Systems for Battlefield Command and Control* (London: Brassey's UK, 1989), 238.

20. Andrew F. Krepinevich, Jr., *The Military-Technical Revolution, A Preliminary Assessment* (Washington, D.C.: Office of the Secretary of Defense/Office of Net Assessment), 6.

21. Lt Col Mark C. Lewonowski, USAF, *Information War*, Essay presented to the faculty of Air War College in fulfillment of the curriculum requirement, Air University, Maxwell AFB Ala., 1991, 29.

22. Rice and Sammes, 152–53.

23. This system was explained to me by Maj Dean Irving, SSC/SSF, USAF Communications Command, Maxwell Air Force Base, Ala., Gunter Annex, in a discussion about the future of C^3I systems, 15 April 1993.

24. *Conduct of the Persian Gulf War*, 574.

25. Air Force Manual (AFM) 2-25, initial draft, "Air Force Operational Doctrine, Space Operations" (Washington D.C.: Department of the Air Force, HQ USAF), April 1993, 23.

26. Stares, 163.

27. *Conduct of the Persian Gulf War*, 151.

28. United States Space Command Operations Desert Shield and Desert Storm Assessment(U), January 1992, US Space Command, Peterson AFB, Colo. (SECRET/NOFORN), information extracted is unclassified, 4.

29. Pierce and Noll, 192.

30. John R. Doner et al., *Distributed Network Vulnerability Assessment (DNVA)*, Harris Corp., Final Report RADC-TR-89-273, vol. 1 (Griffiss AFB, N.Y.: Rome Air Development Center, Air Force Systems Command, January 1990), 12–13; and Andrew S. Tanenbaum, *Computer Networks* (Englewood Cliffs, N.J.: Prentice Hall, 1989), 15, 196, 271, 371, 472, 528.

31. Report RADC-TR-89-341, G-7.

32. Report RADC-TR-89-273, vol. 1, 28.

33. Ibid.

34. Anthony C. Brown, *Body Guard of Lies* (New York: Harper and Row Publishers, 1975). Brown describes in detail how the use of ULTRA to send false force size and intentions to Germany convinced Hitler that the main Allied Cross Channel invasion would land at the Pas de Calais. This resulted in the Germans keeping their forces dispersed and out of position to meet the amphibious assault at Normandy. Brown estimates that due to the success of the misinformation campaign, the Allies saved 60,000 lives.

35. Report RADC-TR-89-273, vol. 1, 65.

36. Physical attack causing equipment damage may be accomplished with either high explosive weapons or damaging nonlethal weapons such as EMP or microwave bursts which can destroy electronic wiring and circuits.

37. Report RADC-TR-89-273, vol. 1, 15.

38. Ibid.,17.

39. Ibid., 32.

40. Ibid., A-1 through A-13.

41. William J. Broad, "Russia Is Now Selling Spy Photos From Space," *New York Times*, 4 October 1992, 10.

42. Report RADC-TR-89-273, vol 1, 65.

43. Report RADC-TR-89-341, 16.

44. Ibid.

45. Report RADC-TR-89-341, 18.

46. A Defense Sand T Intelligence Study, *Electronic Warfare Threat to the U.S. Satellite Communication Links—USSR*, Report DST-26105-111-91, Defense Intelligence Agency, Department of Defense, 20 March 1991, 72.

47. Report RADC-TR-89-341, 16.

48. Ibid., 19.

49. Ibid.

50. Mark W. Eichin and Jon A. Rochlis, *With Microscope and Tweezers: An Analysis of the INTERNET Virus of November 1988* (Cambridge, Mass.: Massachusetts Institute of Technology, 1989), 10.

51. Rice and Sammes, 235.

52. Ibid., 236.

53. Stares, 204.

54. Report RADC-TR-89-273, vol. 1, 43; and James Gleick, *Chaos, Making a New Science* (New York: Penguin Books, 1987).

55. Report RADC-TR-89-273, vol. 1,43.

56. John R. Boyd, *Organic Design for Command and Control*, Document M-U 43947-2, Air University Library, May 1987, 26. Also, Soviet doctrine states that a two-thirds degradation of communications would allow them tc operate ahead of their enemy's decision loop.

57. Secure Solutions, Inc., *Placement of Network Security Services for Secure Data Exchange*, SBIR Topic Number N91-061 (La Jolla, Calif.: Secure Solutions, Inc., 1992), 2-5 through 2-9.

58. Rice and Sammes, 233.

59. Report TADC-TR-89-341, 8.

60. Ibid., 8–9.

61. Ibid., 11.

62. Ibid., 11–12.

63. Ibid., 11.

64. Ibid., 12.

65. Tanenbaum, 287.

66. Lt Col Pat A. Pentland, "Center of Gravity Analysis and Chaos Theory" (Unpublished research report, Air War College, Air University, Maxwell AFB, Ala., April 1993), 17. In his COG analysis, Pentland describes the robustness of modern systems. He states that "the effect of a single type of power is rarely persuasive if used independent of other type power, and influence is magnified when the various elements of power are used in combination rather than in isolation." This concept also applies to attacking a system with a mix of weapons and strategies.

67. Giulio Douhet, *The Command of the Air* (Washington, D.C.: Office of Air Force History, 1983), 30.

68. Dateline, *Are Your Secrets Safe*, NBC Television News program, transcript produced by Burrelle's Information Service, Box 7, Livingston, N.J. 07039, 27 October 1992, 12.

Chapter 3

Disabling Weapons

Cleary's aerospace plane was ninety seconds into a correctional rocket burn when all his cockpit electronics went dead. . . . He didn't have a single working computer on deck. And then he admitted it: they had been pulsed. . . . A pulse beam could have destroyed every piece of working or connected electronics on the X-NASP, if the pulse was quick enough and strong enough to get past the suicide switches.

—Daniel Stryker
Cobra

The above scenario may sound as if it was from an incredulous "sci-fi" novel, however, to others it is reality. The weapon which Cleary describes is within the grasp of today's disabling technologies. America's national science laboratories are among those who recognize this reality and are currently theorizing, developing, and testing these next generation of weapons, thereby transcending the precision guided munitions (PGM) used in the Gulf War.[1] Nonlethal technologies are the only way to fully exploit telecommunications, and depending on campaign objectives, they may be cheaper, more effective, and less destructive. In extreme cases, when conventional weapons are prohibited, nonlethal technologies may be the only alternative.

These technologies have recently gained great appeal in the domestic and international political arena. Editorials and other strategic publications routinely specify disabling weapons (DW) as a mechanism to solve political problems requiring military force.[2] Much of their popularity emanates from a potential to influence problems across the spectrum of conflict range while promising effective but less lethal force. Defusing the illegal drug trade, slowing the proliferation of weapons of mass destruction, and stopping the ethnic cleansing in Bosnia are just some of the crises in which the use of nonlethal technologies are being considered.

In 1970 Joseph F. Coates conducted research on the application of nonlethal weapons during conflict for the Institute for Defense Analysis, Science and Technology. His findings are appropriate for the world order of today. He concluded the requirement for less lethal military capabilities are needed to:

> enable US forces to act effectively in various political-military roles and missions. The general increase in insurgency, increased with the anticipated increase in benign and quasi-military missions, suggest the requirement for less destructive, less deadly tactics and devices than are now conventional.[3]

While somewhat prophetic in his findings, today's use of nonlethal weapons (NLW) can be a force multiplier throughout the spectrum of conflict. This is especially true when employed against digital telecommunication systems. It provides the planner with the tools to fully exploit the high-tech information systems used on the modern battlefield. And, because of the rapid proliferation of high-tech systems, development of disabling technologies can help maintain the US's dominance over the information wars of the future.

In a narrow sense, this chapter will identify what type of nonlethal technologies apply specifically to the exploitation of communication and information systems. This is especially important because one of the greatest potential applications of NLWs is against these two target sets. However, in a broader perspective, this chapter will also familiarize the reader with the overall concept of nonlethal technologies so that he understands the factors affecting their development and use.

I will begin by defining nonlethal technologies. An accurate definition is important because a misperception of the principles behind nonlethal weapons may bias the way one thinks about, and hence employs these weapons. After defining nonlethal technologies, I will provide a brief history of their use followed by some of the legal considerations affecting their development and employment. The legal aspect of employment may prove to be a roadblock for the use of some of the technologies. I will then differentiate between the kill mechanisms of conventional and nonlethal weapons. This area will also list some of the current technologies being explored. The final section will identify when to use these technologies against communications and list some of their advantages and disadvantages.

Definition

In many respects the term *nonlethal* as it applies to weapons is somewhat of a contradiction in terms. It is difficult for many to agree to a common definition because the term nonlethal weapon conjures up the image of attacking someone or something without causing death or destruction. While this is the intent of using these weapons, they do have the capacity to kill and destroy either directly or indirectly. Therefore, it would be more accurate to say they have *potential* to reduce the death and destruction which more conventional methods of blast, fragmentation, and fire usually cause. They can also create conditions which to facilitate death and destruction, or they can cause long term disruption as a result of their indirect effects. For example, an electro-magnetic pulse fired at a nation's telecommunications system may provide an advantage for follow-on lethal attacks. But, it may also result in large scale death due to indirect effects on a society's electrical grid. Therefore, some choose to replace the term nonlethal with other monikers more reflective of the weapons effects. These include "disabling weapons," "low lethality weapons," and "low collateral damage munitions."

In May 1991, an Under Secretary of Defense policy planning group described nonlethal weapons as "an instrument designated to achieve the same tactical or strategic ends as lethal weapons, but which are not intended to kill personnel or inflict catastrophic damage to equipment."[4] This definition captures the essence of nonlethality, but it is somewhat limiting. Los Alamos National Laboratories, who are currently developing nonlethal technologies, expanded on the above definition. They cite three goals for the application of these technologies:[5]

1. no unintentional loss of human life;
2. controlled levels of physical damage; and
3. expanded options for commanders.

After reviewing much of the literature written on nonlethal technologies, I arrived at the following definition: nonlethal weapons include nonconventional weapons technologies which disrupt, degrade, or destroy (or enhance the ability of other weapons to do so) enemy capabilities throughout the conflict spectrum, and whose intent is to prevent or reduce loss of life or catastrophic destruction of equipment. However, depending on the situation and type of technology used, direct or indirect loss of life and damage to equipment may result from their employment.

Assigning a name to this definition is more difficult than developing the definition itself. The terms *nonlethal* and other monikers are clearly inaccurate and may present undesirable public and international sentiment when nonlethal attacks result in even one death. While the term *disabling* describes a desirable effect of all type weapons, it best describes the attributes and intentions of nonlethal technologies. It also connotes an image which differs from conventional, unconventional, or nuclear weapons. Therefore, I will use the term *disabling weapons* (DW) throughout the remainder of this thesis.

History and Legal Considerations

The concept of disabling technologies is not a new phenomenon. In ancient times, adversaries had little variety in how to employ their forces. Limited technology generally required direct force on force battles and greatly reduced the number of ways one could even do that. There were no telephone lines to exploit, electricity to deny, or fuel to contaminate. However, nonlethal methods were devised to aid a commander in either his attack or retreat. One such method was the use of smoke to deceive the opponent to the whereabouts of his enemy. If successful, the smoke would surprise the enemy and provide a positional advantage. In addition, the enemy would use smoke as an asphyxiating agent to aid in siege warfare.[6]

During World War II and the Vietnam conflict, disabling technologies began to come of age. During the Battle of Britain, the British discovered that the Germans were using electronic directional beams to guide their bombers to the target. To disrupt the targeting solution, the British used electronic

countermeasures to override the German navigation signals causing the Luftwaffe to "completely miss the city of London with their bombs."[7] In Vietnam, false targets were inserted into air defense radars creating confusion among the controllers and causing them to misvector attack aircraft.[8] During the same conflict American forces resorted to the use of what they thought to be nonlethal chemicals such as "Agent Orange" to defoliate the dense jungle canopy in order to expose enemy forces and lines of communications.

More recently, *Aviation & Space Technology* reported that during the Gulf War Coalition forces used numerous disabling technologies. One most highly publicized for its effectiveness and consideration for minimizing long term damage was the Tomahawk cruise missiles filled with carbon-fiber threads used to attack electrical generation plants. The attacks were successful and resulted in massive short circuits causing "immediate shutdown of the huge, hard-to-replace generators but [caused] no damage."[9] As a result of the success of both DWs technologies and precision guided munitions in reducing loss of life on both sides (especially civilians), the public and politicians demand even fewer casualties in future conflicts. Ironically, however, some of the technologies that measure up to these demands have come under close legal scrutiny.

While there is no indication that disabling weapons would violate the concept of *jus in bello* (justification for war), there is concern over their implications to *jus ad bellum* (actual conduct of the war). Specifically, for *jus ad bellum*, there are numerous protocols, agreements, and common law beliefs which some types of DWs may be interpreted as violating. The majority of these restrictions, however, apply to the use of chemical or biological agents.

Some of the restricting guidelines come from the 1925 *Geneva Protocol* prohibiting the use of chemical (CW) or bacteriological (biological) weapons (BW), the 1969 US unilateral denouncement of the use of BW and first use of CW, the 10 April 1972 convention on the *Prohibition of Development, Production and Stockpiling of Bacteriological and Toxin Weapons on Their Destruction*, and the 1977 convention on the *Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*. Even if a particular technology is not specifically prohibited by one of the above protocols, many are concerned that their use will cause escalation towards more deadly chemicals or bacterial warfare. One of America's foremost strategist makes the statement "there is a simplicity to 'no gas' that makes it almost uniquely a focus for agreement when each side can only conjecture at what alternative rules the other side would propose and when failure at coordination on the first try may spoil the chances for acquiescence in any limits at all."[10]

One renowned international lawyer states that problems exist as to the legitimacy of nonlethal chemical weapons and in "recent negotiations great attention has been attached to the degree of lethal effects of chemical

weapons. There has been little agreement on the . . . types of nonlethal chemical weapons which many states consider essential to warfare."[11]

However, some biological and chemical agents are beginning to receive favorable attention in the international legal community. As these agents prove their safety to people and the environment, they will be more readily accepted. For example, some agents currently under development to dissipate oil spills could also be acceptable in warfare. Some agents have already been used in the commercial market for years in products such as household carpeting.[12]

Also jeopardizing the development of DWs is the efforts of special interest groups. Some in the international legal community have attempted to restrict the development and use of "questionable" or "dubious" weapons. They claim some DWs fall into these categcries.[13] However, their interpretations are not legally substantiated. As long as weapons comply with the concepts of discrimination (laws of noncombatant immunity) and proportionality (degree of destruction compared to objective obtained), the US needs to refrain from the pressure from these groups and develop whatever legal weapons best protect our national interests.[14]

Overall, the major dilemma concerning the use over DWs is that technology has outpaced the laws of war and is acting as an inhibitor to their development and use while at the same time the public demands less lethal means be used to settle conflicts. A closer look at what differentiates conventional and nonlethal kill mechanisms may illustrate why some nonlethal technologies generate legal concern.

Conventional and Disabling Kill Mechanisms

When using conventional weapons, a typical problem is how to effect just the equipment inside a particular facility. Attacks normally result in destruction of both the equipment and the building. The conventional Joint Munitions Effectiveness Manuals (JMEM) clearly identify the likelihood of undesirable collateral damage and that the "development of reversible nondestructive measures for neutralizing facilities could, in many situations, be of value."[15] With nonlethal technologies, it is no longer necessary to "blow up" a particular target. This is especially true now that the equipment necessary to compete on the modern battlefield has working tolerances which "are much tighter, they are more dependent on timely accurate intelligence as well as command and control, and there are simply more things that can be caused to malfunction."[16] Therefore, this section will provide a framework for the planner to consider when selecting which type weapon to use to achieve campaign objectives against communication systems.

The section begins with an explanation of kill mechanisms and damage criteria. It then presents a model that helps analyze which weapon to select based on various factors affecting the campaign. In this process, I will list some of the kill mechanisms of both conventional and nonlethal weapons.

Damage criteria is "related to the function of the target and is the level of damage that renders the target incapable of performing a specific function."[17] An example of damage criteria can be related to a communications network. The level of damage desired may be to achieve a 90 percent degradation in all telecommunications for the duration of the conflict, or to render them inoperative for only one hour. In the case of the former, one may need to attack the system with conventional weapons turning it into rubble. For the latter requirement, jamming key nodes, firing microwave blasts at transmission or reception antennas, manipulating system information, or inducing a virus into the software may suffice. In either case, the planner should consider the synergistic effect of using both conventional and disabling weapons.

The damage or kill mechanism of the weapon is defined as the "phenomena by which the weapon inflict[s] damage on the target. . . ."[18] In the case of conventional weapons the mechanism may be fire which changes the composition of the target. For a particular nonlethal mechanism, it may be a chemical which crystallizes rubber tires or shorts out circuits. Selecting the most appropriate mechanism depends on the judgment of the planner. Figure 13 provides a framework to aid planners in determining the appropriate weapon(s).[19]

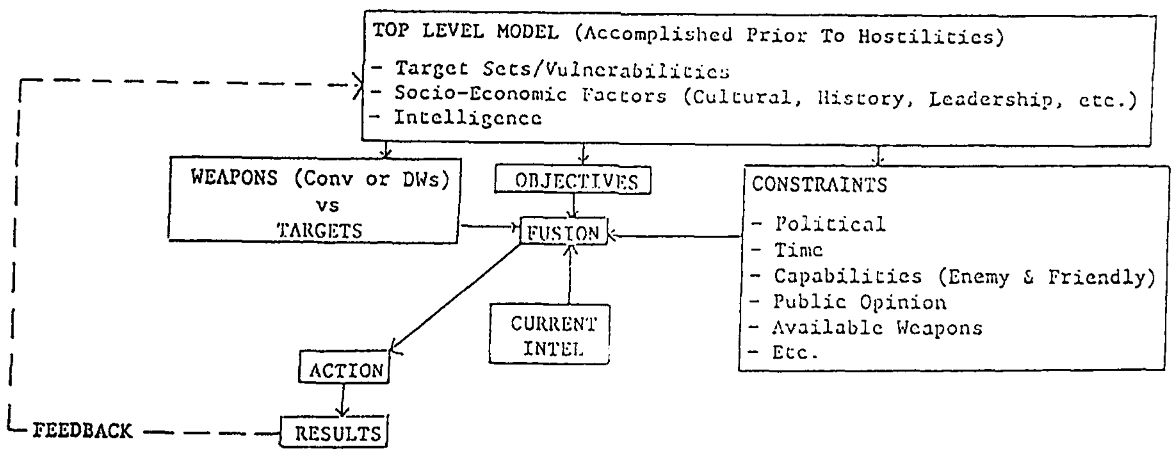


Figure 13

Figure 13, while not all inclusive, does emphasize that the overall attack plan is a function of numerous variables in which weapons selection is only one. However, before making that selection, systems must first be analyzed for vulnerabilities.

When determining vulnerabilities on a macro scale, the analyst should account for the damage caused by an attack to "all systems, not just combat systems and not just the primary objective of the fire."[20] It may be that centralized control of an air defense system, as with the Iraqi system used in Desert Storm, is totally dependent on telecommunications, thereby, an attack

on telecommunications may also disrupt the defense system. However, when analyzing just a particular system, the same principle reapplies in that every system is made of many parts or subsystems. To determine vulnerabilities JMEMs recommends three steps:[21]

1. functional analysis—identify the function of each part of the target and establish relative importance, and then "designate those vital to its operation and those whose destruction would achieve the objective of the attack." For example, identifying the air-conditioning unit of a computer complex as a critical component or the multiplexing unit of a telecommunications switching station.
2. physical vulnerability analysis—this "includes construction types and overall dimensions of structures and equipment, material of construction . . . and other pertinent factors." Of particular interest for the use of DWs would include factors such as the computer network layout or hardening of electrical equipment to EMP.
3. sources of information—"information for both the functional and physical vulnerabilities analysis may be derived from such sources as aerial photos, reports of espionage agents, insurance contracts, business prospectuses, and POW interrogations." Publications and industrial experts can also provide valuable intelligence.

It should be apparent that these considerations closely resemble the process I developed for communication systems and applied in chapter 2. Once the analysis is completed and the objectives are clear, the planner can then select the method of attack based on the available weapons technology and the imposed constraints. The following five steps assist the planner in this selection:[22]

1. define vital components;
2. identify vulnerabilities and determine damage criteria;
3. select wepons capable of achieving damage;
4. evaluate method and accuracy of delivery; and
5. determine capability to measure effects of attack (battle damage assessment).[23]

Now that the foundation for thinking about how to select a weapon has been laid, I will provide a list of the four primary kill mechanisms for conventional weapons and some of the mechanisms now available or being considered for disabling weapons.

Although the objective of an attack against communications may not be its destruction, it is the normal result, desired or not, of using conventional mechanisms. There are four primary kill mechanisms associated with conventional weapons. A single bomb may contain all four, or be designed to take advantage of one or a combination of mechanisms, depending on target vulnerabilities and damage criteria. The mechanisms include:[24]

1. blast—high over pressure creating shock such as that found in a fuel air explosive weapon.

2. penetration—a bomb or fragments of jagged steel produced from the bomb casing exploding or special devices inside the casing that penetrate the target breaking the system or its subsystems.

3. crater—violent earth shock breaking up smooth surfaces or damaging them such that the surface becomes unusable (e.g., a runway). This is the result of penetration and blast.

4. fire—fire damage caused by the weapon and then fires fueled by target material itself with radiant heat igniting combustibles to melt and damage components/things.

As alluded to earlier, for a kill mechanism to be effective, it might not have to destroy the target if it can eliminate or reduce performance "of one or more of the critical functions of the target system."[25] With the use of DWs destruction is not always necessary. For example, at the strategic level if one's intent is to deny the enemy intelligible communications, a disabling weapon may be able to misroute all information rendering a system useless while still providing the attacker a source of SIGINT. The following is a list of just some of the disabling technologies and their kill mechanisms either available or currently being considered.[26] This list should illustrate to the reader that imagination is a key factor in developing and employing these technologies.

MECHANISM	*EFFECT*
Combustion chemistry	– shut off/overspeed engine – contaminate fuel
Polymer chemistry agents	– damage vital components (e.g., air filters) – polymerize fuel system – depolymerize plastics and electrical components – runway and roadway slippery/stick – damage power grid (colloidal dust)
Antimateriel biological agents	– thicken fuels – dissolve electronics, plastics, solder, and other substances
Superagents, acids, oxidizers, and solving agents	– damage tires – disable mines – blind optical ports/sensors
Computer viruses or worms and fire	– subvert communications, radar, satellite, and computer signals control operations
Electro-magnetic pulse (EMP)	– damage communication systems – explode ammo dumps

Blinding lasers	– blind optics, dazzle operators, overload tracking and targeting sensors
Neural inhibitors	– short circuit human synoptic pathways
Calmative agents	– tranquilize personnel
Infrasound	– sound projection to disorient, sicken, or frighten people from designated areas
Holographs	– psyops to convince adversaries to act in desired manner

While this list reveals a number of interesting concepts with which to attack enemy communications, there are both advantages and disadvantages to their use.

Advantages/Disadvantages

The US Global Strategy Council states that "nonlethality is an essential strategy for the future" and that "the opportunity for the US is incalculable."[27]

While the word "essential" may overstate the council's case, under certain conditions nonlethal/disabling technologies do provide advantages over conventional weapons. These advantages fall within three categories. First, they expand US ability to act throughout the spectrum of conflict (fig. 14).

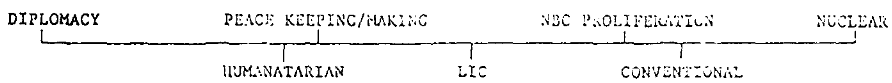


Figure 14

Therefore, a major advantage of a disabling strategy is that it will increase "the number of options for decision makers at the lower end of the conflict spectrum, while increasing military effectiveness at the higher levels of the operational continuum."[28]

At the lower end of the spectrum, one could manipulate information controlling the economic resources of a country prior to hostilities, or intercept communications to assist in locating and interdicting illegal drugs. At the higher end, a full exploitation of command, control, and communications, to include destruction of the national telecommunications network, may be desirable. For example, during Desert Storm "the use of disabling weapons could have denied Saddam his biggest propaganda victory of the Gulf War—the 13 February 1991 bombing by an F-117 fighter of Al Firdus Bunker, which killed scores of civilians."[29] As in this case, disabling technologies may allow you to act where as before inaction may have been chosen due to response options.[30]

Second, the use of disabling technologies can enhance American political reputation and thereby permit prosecution of the war to attain original political and military objectives. This reputation is primarily realized by reducing military and civilian casualties and limiting property destruction. The primary driver behind this is the public opinion influenced by the media.

In a School of Advanced Airpower Studies (SAAS) 1992 thesis, the author convincingly points out that the extraordinary power of the media to shape and orchestrate "not only public opinion, but also public policy."[31] The change in targeting policy resulting from television coverage of the Al Firdus Bunker bombing during Desert Storm is evidence of this power. However, if an adversary decides to put civilians in a critical command, control, and communications facility, then it is he who must take the blame for their deaths. The point is that until a disabling weapon can effectively take out a critical target such as that mentioned above, the US should not refrain from using conventional weapons, especially if the adversary is closely matched. In many cases, the US would be justified morally and legally to take such action, however, past conflicts show we normally do not. The reason for inaction is often fear of the media.

Some argue that reducing the calamities of war will also reduce the deterrent effect that visual, violent death and destruction may have on an aggressor nation's decision to initiate war. A professor at SAAS stated in a point paper that as a result of the media and politics, the third world may attempt to negate US technological superiority.

> There evolves a specious division between public and private morality and accountability. As a result, "the people" are "victims" in every respect—they are "victims" of their own government and they are "victims" of errant American bombs. Legal and moral accountability is thrust back on the attacker who remains on the defensive in the eyes of international opinion.[32]

This professor continues by saying that although reeducation of the public about the realities of war would help, international pressure will continue to demand less lethal warfare, limiting acceptable legal and moral military options. While absolved to the fact that the US will eventually succumb to these pressures, he offers one method of meeting the demands of this new paradigm—develop disabling weapons technologies.[33]

The third advantage is that in certain conditions or against some target sets, disabling technologies may prove more effective than conventional weapons. For example, if during Desert Storm it was necessary to attack the numerous Iraqi telecommunication nodes protected by their location in hotels and along the oil pipeline, disabling weapons may have provided the ability to more fully exploit the system.

In short, there are numerous advantages DWs offer to both the strategist and tactician throughout the spectrum of conflict. If employed imaginatively, and in the appropriate situation, they can maintain the deterrence value of US military capability and help prevent the premature curtailment of military operations prior to the attainment of political objectives. Although

advantages of using NLWs abound, there are some disadvantages associated with their use.

There are two major categories that disadvantages fall into. The first is that technology has not yet caught up to the expectations of what disabling weapons promise. Many of the technologies are at the stage where further research and development is necessary to prove their value. The second category deals with the negative consequences of their use—for instance, would their existence unnecessarily result in US involvement. Let's first discuss the technology issue.

One of the major concerns of most commanders is the effectiveness of disabling weapons. It is one thing to say we will insert a virus into the telecommunications system and expect to see the air defense system disrupted. It is another to actually achieve those results within the desired time frame. This question leads to the biggest concern.

How do we measure the effects of their use. Current ability to measure conventional battle damage assessment is marginal. Ability to measure nonlethal damage is unknown. How will we determine if the virus has sufficiently affected the air defense system so that the lethal attack on it can be initiated with minimal threat to the attacking aircraft? Or even more optimistically, can we determine if the system needs to be attacked with lethal weapons at all? If we misjudge our effectiveness, a disabled soldier or system may more readily reappear. In addition, an impaired system can sometimes continue to operate at some level and, therefore, contribute to enemy combat effectiveness.[34] There is no doubt that existing BDA capability is insufficient.

On the other hand, some disabling weapons currently may be too devastating. A "large footprint may create unwanted area denials, and may affect large numbers of targets, including some outside the immediate battle area."[35] The inability to contain a computer virus to just a particular system or prevent it from spreading to friendly systems is a significant problem which will limit its use. Another example of collateral damage is the use of an EMP blast which affects the entire electrical system of a city instead of just the electrical components inside a telephone exchange.

A problem exacerbating all the above disadvantages is how to deliver disabling weapons. It is this area in particular that has had the least amount of thought. More than anything, this illustrates a certain lack of doctrinal thought towards the whole subject of DWs. Also important to doctrine are the consequences of using disabling weapons.

Topping the list in this second category is the potential for escalation. Two areas of concern present themselves here. First, the attractiveness of DWs may encourage increased US intervention into international conflict.[36] Because they promise to be precise, nonlethal, and potentially covert, many may misuse them as a panacea to solve any problem where lethal means are not desirable. The second area of concern is that the use of disabling weapons, even in their most benign form, will most likely be considered as an act of war or sabotage, thereby causing the opponent to escalate. A possible result of the

combination of these two concerns is that the US may become involved in a lethal conflict it originally had no intentions of entering.[37]

There is also a legal issue. As mentioned earlier in this chapter, many believe that "nonlethality could pry open a Pandora's box of chemical, biological, and nuclear weaponry that diplomats have spent much of the twentieth century trying to keep closed." [38] Not only will these type weapons meet resistance within the international legal community, but they may also lead to the enemy propagandizing the "autarchy" of their use.

Finally, highly technical societies are very vulnerable to disabling technologies, therefore, developing such weapons could provide third world countries a cheap means with which to attack the US. In the near future, one may see the computer as the terrorist's weapon of choice.

While some of these disadvantages seem significant, one must remember that DWs do not replace conventional methods, but provide commanders additional and complementary options throughout the spectrum of conflict. The above disadvantages are not impossible to overcome, however, expanded research and development is necessary. In addition, policymakers must understand that the use of disabling weapons is an act of war just as surely as using lethal weapons. Ultimately the decision to employ disabling weapons must reside with the policymaker and the campaign planner based on the current technologies and the situations they face.

Conclusion

Disabling technologies have great potential for future conflict, especially against command, control, and communication systems. However, a coherent, joint doctrine to guide their development and employment is lacking. Many politicians and military policymakers have little understanding of the potential capabilities, limitations, and employment strategies of disabling weapons. For example, do we employ them before, during, or after hostilities; do we employ them in conjunction with lethal weapons or use them separately; which technologies show more promise for the future; how will we deliver them? The military services most likely to play a leading role in future conflicts will be those who have thought about how to use these new technologies and incorporated them into their acquisition and training programs.

I described how disabling technologies can help exploit telecommunications, and laid a foundation for the development of a coherent doctrine incorporating the use of disabling weapons. I emphasized educating potential users to the capabilities of disabling technologies. In doing so several areas were discussed. First, a working definition was developed to better understand the purpose of DWs and to generate mission needs and strategies. Second, a brief history of DWs pointed out that their use dates back to wars of antiquity and illustrated some of the legal problems associated with their use. Third, this chapter differentiated between lethal and nonlethal kill mechanisms in order to stimulate discussion on how to use both for a more effective military

strategy. Finally, it highlighted some of the primary advantages and disadvantages of disabling technologies.

However, the overall message this chapter sends is that disabling technologies can make a significant contribution to US strategy and our capability to control information warfare. Disabling weapons should be pursued with greater enthusiasm, especially by the Air Force. A recent DARPA report agreed with this recommendation. It stated the US pays too much attention to lethal munitions, and that in some cases, nonlethal technologies may be more effective. Ignoring nonlethal munitions programs will limit US capability to respond to future conflict and to deter potential opponents.[39] This is particularly relevant to C^3I control in war.

I close this chapter by offering a warning that Alexander de Seversky gave to the Air University in 1948: "Unless you plan your strategy and tactics far ahead, unless you implement them in terms of the weapons of tomorrow, you will find yourself in the field of battle with weapons of yesterday."[40]

Notes

1. Briefing given to SAAS by John Alexander from Los Alamos National Laboratories, September 1992. Alvin Toffler as stated that the precision weapons of the Gulf War represented the "third wave" of warfare, while others look at the future potential of nonlethal weapons (NLWs) and describe them as the "fourth wave." Some go further and cogitate nonlethality as advancing warfare to the point where war can be conducted against an adversary without his knowledge of it.

2. Michael J. Dugan and George Kenny, "Operation Balkan Storm: Here's a Plan," *The New York Times*, 29 November 1992, E-11.

3. Joseph F. Coates, *Nonlethal and Nondestructive Combat in Cities Overseas*, Paper P-569, DAHC 1567 C 0011, Task T-62 (Arlington, Va.: Institute for Defense Analysis, Sciences and Technology Division, May 1970), 105.

4. Capt Mark D. Martin, USN, *Non-lethal Weapons: A Policy Planning Paper*, Office of the Under Secretary of Defense, Policy Planning Division, 29 May 1991, 1.

5. Alexander briefing.

6. Martin van Creveld, "The Persian Gulf Crisis of 1990-91 and the Future of Morally Constrained War," *Parameters* 22, no. 2 (Summer 1992): 27.

7. Defense Advanced Research Projects Agency (DARPA), *Assessment of Mission Kill Concept, Requirements, and Technologies*, Final Report SPC 1361, SPC Log No. 90-1987, September 1990, 6.

8. John R. Doner et al., *Distibuted Network Vulnerability Assessment* (DNVA), Harris Corp., Final Report RADC-TR-89-273, vol. 1 (Griffiss AFB, N.Y.: Rome Air Development Center, Air Force Systems Command, January 1990), 28.

9. David A. Fulghum, "Secret Carbon-Fiber Warheads Blinded Iraqi Air Defenses," *Aviation & Space Technology*, 27 April 1992, 18.

10. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press, 1966), 131. His statement here is specifically speaking about use of lethal gas. However, the concept he raises is that once a weapon is allowed, the limits of its use are both difficult to agree upon and have potential for escalating to more lethal means. As he says in the same paragraph, "some gas raises complicated questions of how much, where, under what circumstances; no gas is simple and unambiguous."

11. Shelton M. Cohen, *Arms and Judgement* (Boulder, Colo.: Westview Press, Inc., 1989), 224–225.

12. Dr John B. Alexander, Chief of Los Alamos National Laboratory's Nonlethal Weapons division, telephone discussion with author, 21 April 1993.

13. Miguel D. Walsh, *New Technology, War and International Law*, Unpublished Paper, June 1991, 20.

14. For further explanation of these two rules see W. Hays Park, "Air War and the Law of War," *The Air Force Law Review* 32, no. 1 (1990): 4 and 168.

15. Coates, 33.

16. DARPA Report SPC 1361, 7.

17. Joint Munitions Effectiveness Manuals (JMEM), USAF Fighter Weapons School Instructional Text, Courses F4000IOAN, A1000IDOPN, F1600IDOPN, F1500IDOPN, Part 1, June 1982, 4–3.

18. JMEMs, 4–3.

19. The model was developed during a brainstorming session which I attended at Los Alamos National Laboratories, 15 October 1992.

20. DARPA Report SPC 1361, 31.

21. JMEMs, 4–2.

22. Ibid., 1–3.

23. This is my own addition to the list of JMEMs recommendations. This is an especially important factor when considering the employment of NLWs since their effects are not always visible. Not being able to measure effects would be one of the primary reasons to dismiss a DW as the primary attack weapon.

24. JMEMs, 3–1.

25. DARPA Report SPC 1361, 8.

26. This list was derived from Captain Martin's policy planning letter and Janet Morris, *Nonlethality Briefing* (Washington, D.C.: US Global Strategy Council, 1991).

27. Janet Morris, *Nonlethality Briefing*.

28. Memorandum, John C. Hopkins, Los Alamos National Laboratories, subject: Nonlethal Strategy Group Meeting with the USN, 20 September 1991, 2.

29. Andrew Weinschenk, "Army Gives a Boost to Exotic, Non-Lethal Weapons," *Defense Week* 13, no. 41 (19 October 1992): 1, 9.

30. Lt Col Alan W. Debban, Headquarters USAF, "Disabling Systems: War-fighting Options for the Future," *Airpower Journal* 7, no.1 (Spring 1993): 46.

31. Lt Col Marc D. Felman, "The Military/Media Clash and the New Principle of War: Media Spin" (Master's thesis, School of Advanced Airpower Studies, 1992), 5.

32. Peter R. Faber, "Our Quarrel Is with the Regime, Not the People Argument," (Unpublished point paper, School of Advanced Airpower Studies) written in response to a briefing given by Col John Warden, commandant of Air Command and Staff College, about how future war must be less lethal to both civilian and military personnel, 15 September 1992), 1–2. Faber goes on to say that in fact, the people must share the guilt of war with their leader. He states that "even police states require the active cooperation of hundreds of thousands, if not millions, of individuals who do not qualify as passive 'victims'," 1–2.

33. Faber, 3.

34. DARPA Report SPC 1361, 9.

35. Ibid., 7.

36. Thomas E. Ricks, "New Class of Weapons Could Incapacitate Foe Yet Limit Casualities," *The Wall Street Journal*, 4 January 1993.

37. Coates, 101.

38. Janet Morris, *Nonlethality Briefing*.

39. DARPA Report SPC 1361, 11.

40. Alexander de Seversky, "Air Power," a speech delivered before the Air University, 28 May 1948, 5.

Chapter 4

Guidance For Campaign Planning

Many may think that just because we possess disabling technologies we should use them. Contrary to this view, I suggest a more cautious employment strategy when using them to attack telecommunications. Assuming the technology is available to employ DWs effectively (which it currently is not), one must consider that the US is a nation extremely vulnerable to disabling attacks because of its dependency on information. Any use of these technologies may divulge critical national capabilities that many adversaries could then use against the United States. Therefore, they should never be used in a fashion which tips off the enemy to how they were attacked, unless there is an overriding political, economic, or military necessity. This means that the employment of disabling technologies should be masked by deception and combined with the use of lethal attacks when possible. The next section integrates the information from chapters 2 and 3 to provide planning factors to consider when matching weapons to the telecommunications target set. Hopefully this produces the optimum strategy.

Planning Factors

In my research, I found only one document (see appendix B) that addresses factors influencing the selection of one weapon over the other.[1] However, that document is very limited in scope and discusses a broad taxonomy of factors without listing specific conditions to help select the appropriate weapons. Therefore, the following list of 14 guidelines is a synthesis of my own conclusions based on that document and on the information presented in previous chapters. The list does not claim to be inclusive nor recommend strict adherence in all situations. However the planner should consider this list as generic and use it as a catalyst to evaluate the concepts presented by his own circumstances.

1. Knowing the enemy—In other words, do not mirror image. Know how an enemy uses his communications infrastructure. This will provide clues as to which systems he depends on for the various command and control functions and what capacity he possesses to compensate for degradation. The planner should understand that communications form a linkage between an adversary's entire social, economic, political, and military system. Armed with this knowledge, the planner can build his information campaign, and then

study each system to determine which systems are prone to lethal or disabling attack/exploitation mechanisms.

2. Objective—Both lethal and disabling weapons have the capability to destroy electronic and communications equipment. However, as chapter 2 points out, there are numerous ways to exploit communications. Manipulating national economic assets, eavesdropping to gain intelligence, misrouting information, or enhancing a deception plan are just a few. The only way to achieve some of these objectives is through the use of disabling technologies.

3. Intelligence—Intelligence is an issue of kind and quality. With conventional weapons, knowing the location of key nodes, routes, and repair capability is essential to be able to attack with the necessary force to yield the desired effects. Destructive nonlethal attacks such as EMP or microwave blasts would require this same intelligence. On the other hand, disabling attacks using viruses would require additional information about network protocols, command and control of network functions, and how to gain access into the system. Questions such as do different switching stations use different software, and if they do, will the selected DWs achieve the desired effects must be answered. Appendix A gives insight into the type of intelligence necessary to exploit a telecommunications system with disabling weapons. Important to both types attack, however, is an understanding of the systems network dynamics and interaction with other networks.

4. Uniformity—If enough conventional resources can initially be applied to a system and persistently reattacked afterwards, uniformity of effect may be possible. However, because of the quantity and quality of intelligence, offensive resources available, or political constraints one may not always be able to achieve uniformity through lethal means. Therefore, disabling weapons may provide degradation throughout an entire network. Centralization or dispersion of the system is a key function. The more centralized a system, the more vulnerable it is to both lethal and disabling weapons. However, if a system is widely dispersed or decentralized (containing numerous nodes), then selecting disabling weapons to capitalize on their cascading effects may be more cost effective while also achieving a more uniform effect.

5. Restoration—Postcrisis restoration can be expensive for the recovering nation, or for the attacking nation if he chooses to share the cost burden. Precision guided conventional weapons can limit collateral damage, however, when attacking something like a nation's main telecommunication node with high explosives the cost might be prohibitive in dollars and repair time. However, the planner might elect to use conventional weapons if he finds alternative and less expensive nodes or components which still achieve the desired effects. If cost of repair or indirect effects of long term system outages remain a factor, DWs should be considered.

6. Accessibility—As with intelligence, accessibility is also a function of kind. There may be many reasons one could not attack a system with conventional weapons. Political factors, information sanctuaries, location of key nodes in civilian buildings such as a hotel, excessive redundancy,

hardening, or target defenses all reduce the effectiveness of a conventional attack. For DWs these factors are less critical. Access for disabling weapons apply more to the ability of the attacker to infiltrate encryption and other self-protection devices. They also consider system "life-cycle" issues. For example, did the contractor install a fault capability into the system at time of manufacturing which can be activated on demand.

7. Confidence in weapons effectiveness—Conventional weapons have been proven in combat and can be tested and retested. One can reasonably predict not only what will happen to a target when it is hit by a bomb, but also how many bombs it will require to achieve a desired effect. In addition, battle damage assessment is more apparent and better quantified, although PGMs have muddied this issue significantly. On the other hand, the documented success of DWs has a limited sample size, especially in areas typically targeted by conventional weapons. Currently, as target value and threat to friendly lives increase, confidence in the success of DWs decreases.

8. Duration of effects—Once again, the situation dictates the type weapon used. For example, if enough resources can be applied and reapplied to a target set or the system is not very robust to begin with, then conventional weapons could have a long term effect. However, if for various reasons key nodes cannot be attacked or the enemy is able to quickly repair or work around damaged nodes, DWs should be considered. It may be possible for a sophisticated virus to render a system inoperative until reversed by the attacker. In addition, a combination of both type weapons may have a synergistic effect. When considering either type weapon, the speed in which effects occur may be an essential factor.

9. Reversibility—Reversibility of destruction for conventional weapons is usually expensive reconstruction. However, for DWs it may be as simple as pressing a button or as complicated as rewiring an entire national electrical system. It is essential that disabling technologies not be used without knowing the anecdote. To do so could result in spreading collateral damage far outside the target area.

10. Countermeasures—This fits closely with accessibility and duration of effects, and applies to both conventional and disabling weapons. The real challenge is to determine whether or not a countermeasure is effective and if so, to what degree and on what time line.

11. Political effects—These include ability to act overtly, to legally justify a weapon's use, to prevent collateral damage, to accomplish the mission while complying with rules of engagement, or to control environmental damage. Using environmental damage as an example, blowing up an oil pipeline with lethal weapons or changing weather patterns with disabling technologies may be prohibited by international law or self-imposed restraints.

12. Classification of technology—Certain weapons may be too classified to use in a particular situation. The benefit in keeping their existence close-holed may be greater than the ramification of not using them.

13. Delivery vehicle—For conventional weapons it is a function of determining what aircraft or army unit can get to and return from the target.

With DWs, it's more a concern of once access is gained, does the expertise or vehicle exist in order to employ the technology. This is one area requiring greater civil and military cooperation.

14. Escalation control—If the US is determined to respond to a crisis, conventional weapons may more readily prompt an increase in hostilities, whether it be terrorist action or reprisal in kind. Whereas, the ability to act in a disabling fashion with significant enough effects, may coerce a behavioral change without escalating to more deadly and destructive force.

Conclusion

I list 14 factors and conditions that a campaign planner should consider throughout the spectrum of conflict. Although the above factors address many of the correct questions to ask when faced with selecting weapons type and employment strategies, the answers to the conditions are less helpful. I accredit the latter phenomenon primarily to the limited use of disabling technologies in the past and a lack of enthusiasm towards pursuing their future use. When the research into the "demand" for communications is integrated with the "supply" subset, my recommendation becomes more evident. The resistance to pursuing a strong disabling technologies program is somewhat predictable viewed in light of budget constraints which threaten the existence of major weapons systems and force structure. Ironically, budgetary constraint provides one of the strongest arguments for incorporating disabling technologies into our forces.

My research suggests that information is one of the most, if not the most, vital elements of combat capability. While still vulnerable to lethal attacks, the modern telecommunications system is becoming increasingly vulnerable to disabling attacks. Because of these vulnerabilities, and the additional options disabling technologies offer throughout the spectrum of conflict, I recommend a strategy to pursue research, development, and use of these technologies. Since the US is also vulnerable to information warfare, development of a strong disabling technologies program will provide at a minimum a countermeasures capability. It may also result in unanticipated capabilities no one foresees at the moment. However, until disabling technologies improve, it is imperative we employ them in such a way that, if they fail to achieve the desired effects, they do not fail catastrophically. In other words, sufficient lethal force should still be applied to achieve objectives.

Notes

1. Dr John Alexander, director of Disabling Technologies Program, Los Alamos National Laboratories, to Adm David E. Jeremiah, vice-chairman of the Joint Chiefs of Staff, letter, subject: referencing a target matrix to aid in weapons selection relative to conditions applicable to varying scenarios. This matrix identifies targeting factors and lists considerations for each. However, it does not suggest which weapon to select based on that condition. For example, when analyzing the factor of "intelligence," the condition given is "poor-excellent," not "if you have this type of intelligence, one type technology would be more suited than another."

Appendix A

Configuration Perspective

1. Are there critical nodes the loss of which should inordinately degrade network performance?

2. Are there critical geographic areas where a limited amount of ordnance could destroy a large number of nodes?

3. How do pertinent performance parameters change with the loss of increasing numbers of nodes?

4. How do pertinent performance parameters change with the loss of increasing numbers of links?

5. Are there critical links the loss of which would inordinately degrade network performance?

6. Can an adversary jam physical communication links so as to prevent a user from entering traffic when he desires?

7. Do nuclear effects degrade performance on any communication links or communication equipment in the network? Is salvage fusing an effective threat?

8. Is the network dependent on a single or a few links or nodes for message transmission?

9. Can link capacities maintain adequate network performance under heavy load conditions?

10. Which interceptible[sic] parameters are essential for effective use of physical destruction?

11. Can critical nodes be identified, located or prioritized for targeting through analysis of emissions?

12. Can critical geographic areas be identified, located or prioritized for targeting through analysis of emissions?

13. Can traffic levels at each node be determined by observation of the link data stream?

14. Under any circumstances are nodes which otherwise must keep a low spectral profile (LPI) required to provide program uploads to other nodes?

15. Can the network's data link signal transmitters be detected, identified and located?

16. Can an adversary identify communication links or equipment in the network which are most susceptible to nuclear effects?

17. Can emissions be exploited to identify critical links, geographic areas, or time periods for jamming attack?

18. Are any critical links distinguishable by the type or volume of traffic they carry?

19. Which interceptible[sic] parameters are essential for effective use of link spoofing?

20. Which interceptible[sic] parameters are essential for effective use of network spoofing?

21. At what point in the mission is physical destruction effective for any identified susceptibilities?

22. At what point in the mission is jamming effective for any identified susceptibilities?

23. At what point in the mission is link spoofing effective for any identified susceptibilities?

24. At what point in the mission is network spoofing effective for any identified susceptibilities?

Access Perspective

1. What is the relation between link errors (signal distortion), interference power level, and modulation?

2. What are the optimum interference waveform, power levels, and modulation parameters?

3. Can an adversary jam critical communication links?

4. Are frequency division multiplexing techniques used anywhere in the network?

5. Do the frequency division multiplexing techniques allow an adversary to selectively jam portions of the network of interest to him?

6. Are code division multiplexing access (CDMA) techniques used anywhere in the network?

7. Is there any way in which an adversary can increase the difficulty of using CDMA under all network conditions, including simple jamming?

8. Are multiple access techniques employed anywhere in the network?

9. Can an adversary enter information into the multiplexed time assess of CDMA links or is the central multiplexing location a jamming target?

10. Can network emissions be intercepted?

11. What signal parameters can be determined through intercept?

12. Is the generation rate of network entry requests (or invitations) great enough to jeopardize crypto variables, degrade throughput or create a susceptibility to replay?

13. Can user data be interpreted or subtly corrupted by a spoofer who has successfully joined the network?

14. Will the link receivers accept spoofing signals in either sync or information mode?

15. Can an adversary with adequate communication resources enter the network as though he were a friendly network node?

Protocols Perspective

1. What type of automatic repeat request (ARQ) mechanism is used in the network?

2. If Stop-and-Wait ARQ is used, can an adversary lengthen round trip delay by eliminating nodes in order to decrease throughput?

3. Has formal specification and verification been performed on all protocols?

4. Is circuit service provided on any mission critical data?

5. Can segments of mission critical data be delayed or prevented from delivery by jamming one link along a circuit?

6. Can pulse jamming produce inordinate degradation in protocol performance?

7. Can the receiver lose frame alignment and be prevented from recognizing valid frames?

8. What type of link flow control algorithm is used (e.g., Stop and Go, Static Rate, Credit/Windowing, Class, Stop and Wait)?

9. Where "Stop and Go" flow control is used, can an adversary inhibit "stop" control, causing sender to overrun receiver?

10. Where "Stop and Go" flow control is used, can an adversary inhibit "go" control, blocking data from the sender?

11. Where "Stop and Go" flow control is used, can an adversary cause control frames to be delivered out of sequence causing overrun or blockage?

12. Where "Static Rate" flow control is used, can the receiver be caused to change state such that the static rate limitation results in overrun or under utilization?

13. Where "Credit/Windowing" flow control is used, can an adversary block receipt of credits and stop transmission by causing the sender to believe that the window is exhausted?

14. If Go-Back-N ARQ is used, are the transmit and receive window sizes so large as to cause retransmission of an exorbitant number of packets is [if] a single or negative acknowledgments (Nak) is lost?

15. What services are provided on message traffic at each OSI layer in the network? (e.g., circuit service, virtual circuit, datagram, sequenced, reliable...)

16. Can the protocol acknowledgment, retransmission, error detection, or abnormal condition recovery procedures be manipulated to degrade network performance?

17. Where "Credit/Windowing" flow control is used, can an adversary introduce erroneous credits, causing the sender to overrun the receiver?

18. If Go-Back-N or Selective-Reject ARQ is used, can an adversary alter the sequence of received frames in order to cause excessive?

19. If Naks are used in the ARQ scheme (especially in Go-Back-N), can an adversary introduce or replay Naks to induce excessive retransmissions?

20. Is an alternate set of protocols used for program uploads which are simpler and more susceptible to attack?

21. Do countermeasures targeted against higher level forms of attack degrade performance sufficiently to render the network more susceptible to lower level forms of attack (i.e., dummy traffic injection or fixed length frames)?

22. Can the communication service types (reliable versus unreliable, datagram versus connection oriented, sequenced versus nonsequenced) provided to traffic through a particular node be determined by an adversary in order to infer the node types?

23. Can an adversary determine which protocols have not undergone formal verification and exploit this fact to degrade network performance?

24. Can individual messages be identified and distinguished by type, source, destination or priority in the link data stream for the purpose of selective jamming?

25. Can the spanning trees used in broadcast routing be determined from emissions, and used to suppress message delivery to large portions of the network by jamming relatively few links?

26. Can the network layer services provided to host nodes be determined by an adversary?

27. Can any encrypted control data be retrieved at the TRANSEC or COMSEC levels?

28. Can header and control information be identified and interpreted by an adversary? Is header and control data encrypted?

29. Can a knowledge of the protocol services provided at each layer be used to degrade network performance?

30. Can false acknowledgments be introduced to inhibit reliable link service?

31. Can traffic be introduced to upset sequence numbering and acknowledgments?

32. Can an adversary spoof link or physical layer protocols so as to prevent a user from entering traffic when he desires?

33. Can the protocols be induced to enter the initialization or disconnect procedures inappropriately?

34. Can the protocols be prevented from entering the connect procedure under certain conditions?

35. Can protocol parameters be altered resulting in network performance degradation?

36. Where "Message Class" oriented congestion control is used, can a spoofer introduce fictitious high priority traffic, locking out access to other traffic types?

Management and Control Perspective

1. Can an adversary induce deadlock by exhausting message buffer space at a node?

2. Can fictitious data be introduced into routing tables to interrupt data paths, prevent delivery of certain messages, or increase congestion?

3. How dependent is the network on a centralized control facility?

4. Are there direct attack scenarios on communication network assets which can overwhelm computational capacity of network management algorithms (e.g., adaptive routing, adaptive link assignment)?

5. Are there specific node failure rates at which direct attack could undermine network management algorithms?

6. What specific node failure rates cause inordinate degradation of network management algorithms?

7. What is the maximum number of near simultaneous node failures accommodated by the network management algorithms?

8. Can the management and control facility maintain adequate network performance when outages occur?

9. Can the distributed network management coordination technique be undermined by direct attack on network nodes?

10. How are links assigned in the network? Can link assignment be prevented from adjusting to network failures?

11. Can the network congestion control mechanism be disrupted leaving the network or portions of the network locked up?

12. Are any special message transmissions used to establish routing or topology data bases or network management functions (e.g., adaptive routing, adaptive link assignments)?

13. Can selective jamming of special messages used to establish routing or topology data bases disrupt network management functions?

14. Are there jamming attack scenarios which can overwhelm computational capacity of network management algorithms (e.g., adaptive routing, adaptive link assignment)?

15. Can pulse jamming induce oscillations in adaptive routing and delay or prevent message delivery on critical data paths?

16. Are there specific link failure rates at which pulse jamming could undermine network management algorithms?

17. What specific link failure rates cause inordinate degradation of network management algorithms?

18. What is the maximum number of near simultaneous link failures accommodated by the network management algorithms?

19. Can link and node outage reporting be prevented from reaching the management and control facility?

20. Is distributed network management coordination explicit or implicit?

21. Can the distributed network management coordination technique be undermined by increasing bit error rate?

22. At what bit error rate does the distributed network management coordination technique become unsatisfactory (e.g., with respect to adaptive routing and link assignment)?

23. How is message routing determined in the network? Can it be prevented from adjusting to network failures?

24. Are topology or routing updates required at some regular interval, such that jammers could synchronize with this update rate and prevent a node from receiving any topology information?

25. What type of congestion control mechanism is used in the network?

26. Can an adversary provide incorrect network loading information to the congestion control mechanism, decreasing throughput through overloading or underutilization (e.g., can he induce false queue length indications)?

27. Can the network management and control facility detect and respond to abnormal conditions and unauthorized accesses to the network?

28. What information must a node have in order to enter the network?

29. What sequence of events must a node carry out in order to enter the network?

30. Is the active role in network entry ascribed to nodes which are trying to join the network or nodes which are already in the network, or both?

31. Could a node be made to malfunction and overload the network by repeatedly requesting program uploads?

32. Is there any way an adversary can spoof or affect the central network controller in such a way as to degrade the capacity of the network?

33. If the congestion control mechanism uses permits to limit traffic in the network, can an adversary obtain permits, thereby reducing capacity offered to authentic network users?

34. Can the distributed network management coordination technique be undermined by a spoofer entering false control or status information, or by altering or delaying such information?

35. Does the network management and control design have the potential for an external influence to cause disruption of normal network operation through the inappropriate application of controls?

36. Does the network management and control and switching software enforce safe operating limits on parameters and thresholds? Log and report out-of-range requests?

37. Are operator ID's included in all network management and control commands?

38. Are operator ID's verified prior to network management and control command execution?

39. Does network management and control and switching verify that each command is "reasonable" prior to execution?

40. Are directory updates controlled from a central location?

41. Can the directory update procedure be defeated?

42. Are the directory contents verified frequently?

43. Does the network management and control design include provisions for security monitoring?

44. Does the network management and control design have the potential for an external influence to cause degradation of network performance through the consumption of excessive resources invalid but inappropriate management and control activities?

45. Does the network management and control enforce safe limits on: periodic report rate, performance measurement intervals?

46. Does the network management and control design include provision for switching to a backup control element? Can the switch over algorithm be defeated?

47. Do network reconstitution mechanisms adequately adapt to rapidly changing stresses of the network (i.e., jamming, physical destruction, EMP, nuclear propagation effects)? Are these mechanisms susceptible to efforts to prevent the network configuration from stabilizing?

48. Is the network management distributed or centralized? How dependent is network operation on a centralized management and control facility?

49. What network management and control information is maintained at the network management and control facility?

50. What is the effect of delayed, altered, or inhibited network management and control status reports on network performance?

51. What is the effect of delayed, altered, or inhibited control messages sent to network nodes?

52. Are consistent software versions intended to operate concurrently at each node in the network?

53. Can software updates be interrupted?

54. Does the network send out periodic connectivity updates, such that a captured node could be connected and disconnected from the network at some rate, to induce routing or link assignment oscillations?

55. Is ETE encryption employed? Are messages decrypted and reencrypted at gateways?

56. Can power control software be reprogrammed to periodically throttle transmitted power down and up again at a rate matched to adaptive routing or link assignment reaction times, or at inappropriate times?

57. Can traffic be introduced to undermine link status estimators, making heavily loaded links appear lightly loaded or lightly loaded links appear heavily loaded (e.g., early or late acknowledgments)?

58. Can a spoofer compromise the authentication process in order to request a software upload? (Spoofer gains complete copy of network software and has potential for overloading the network with software upload request.)

59. Can a spoofer compromise authentication process in order to provide a compromised software upload to other network nodes? (Could make network totally inoperable or supply subtle access to information in the network.)

60. Can status reports to the management and control facility be delayed, altered, or prevented from reaching the facility?

61. Can control messages sent to network nodes be delayed, altered, or prevented from reaching the nodes?

62. Can the encryption keys and synchronization be tampered with, causing network performance degradation?

63. Can fictitious data be introduced into topology data bases, or link status data bases to undermine adaptive routing or link assignment?

64. How are software uploads initiated?

65. How is a software upload disseminated through the network?

Information Perspective

1. Are there critical network users who would seriously degrade mission performance if prevented from accessing the network?

2. Can critical users of the network be identified by an adversary?

3. Can fictitious or corrupted user data be delivered over the network by a spoofer who has joined the network?

Appendix B

Targeting Factors

Factors	*Considerations*
– Target Value	Low - High – Military – Economic – Social – Political – Psychological
– Accessibility	Easy - Difficult – American Troops/Agent Foreign Agent, Weapon System (Manned, Remote, Spaced-Based) – Time of Accessibility (Life Cycle) – Design & Engineering – Manufacturing – Installation – Prehostilities – Post onset of hostilities – During operation of system – During dormant periods – Strength/Quality of Defense
– Deniability	Required, Desirable, Not Necessary – Nonattributable – Attributed to others
– Damage Required to Disrupt System	Little - Major – Few key nodes – Major damage to primary system – Must take down primary & secondary systems to be effective – Hardware versus software damage

– Damage Detection/Battle Damage Assessment	Easy - Difficult – No detectable damage (System just doesn't work – No visible damage – Hard to detect without special instruments – Physically destroyed (Cinder OK)
– Time to Reaction	Short - Long – Immediate Relatively short (Minutes/Hours) – Relatively long (Days/Months) – Delayed
– Delayed Reaction	Time or Event Triggered – Time – Remote trigger, EM, Acoustic, Shock
– Event	– Parameter change (Temperature, humidity, movement, pressure)
– Policy Implication	None -Extremely Adverse – To US interests in target area – To US interests in other area – To host nation – To target country – To other country/area – Legal issues – Short term versus long term results
– Intelligence	Poor - Excellent – Availability to planners/operators – Current/accurate – Target specific – Ease of obtainability – Timeliness

– Restoration	Easy - Difficult – For the US – For target country – For others – Cost – Time – Material/parts availability – Effects reversibility
– Countermeasures	Easy - Difficult – For US – For others – Ease of detection – Availability
– Technology Sensitivity	Low - High – Initiative lost once used – Not detectable when used (Delivery system destroys evidence) – Masked by other system – Cannot be duplicated
– Control of Effects	Tight - None – Only target location affected – May spread in environment (Air, water, ground, plants, animals, etc.) – Duration (Short to persistent) – Nontargeted substances/items
– Effects Measurement	Easy - Difficult – Externally observable (Human, electro-optics, space-based) – Instrumentation required (EM, IR, acoustic, other sensors) – Sensor system availability – Requirement for confirmation

– Confidence	Low - High – Degree of confidence weapon will produce desired effect – Confidence in operation (Weapon, intelligence, delivery) – Precision of effects
– Delivery Requirements	Easy - Difficult – Accuracy (Small CEP versus general area) – Amount (Size, weight, solid, liquid, gas) – Distance – Weapons system availability – Special requirements (Handling, shielding, etc.)
– Collateral Damage/ Casualty Acceptability	Zero - High – Degree of target isolation – Occupancy of target (Military, government, civilian, third country, hostages, number/demographics) – Time at risk – Cultural factors (Religious, political, social, etc.)
– Environment/Health & Safety Requirements	Mandatory - Waverable (No inherently dangerous weapons)

Bibliography

Air Force Manual (AFM) 2-25. "Air Force Operational Doctrine, Space Operations." Initial Draft. Washington, D.C.: Department of the Air Force. April 1993.

Alexander, John B. Los Alamos National Laboratories. Letter to Adm David E. Jeremiah, vice-chairman of the Joint Chiefs of Staff, concerning a targeting matrix for the use of nonlethal technologies, 6 January 1992.

Alexander, John B., and Andy Andrews. Los Alamos National Laboratories. Meeting concerning nonlethal technologies, 15 October 1992.

_____. *Non-Lethal Defense: A Comprehensive Defensive Strategy Providing Commanders New Options*. Los Alamos National Laboratories. Nonlethal weapons briefing to the School of Advanced Airpower Studies (SAAS), September 1992.

Andriole, Stephen J., and Jon L. Boyes. *Principles of Command and Control.* Washington, D.C.: AFCEA International Press, 1987.

Army Air Forces Evaluation Board Report, Mediterranean Theater of Operations. Vol. 2, 31 January 1945. Historical Research Agency, Maxwell AFB, Alabama.

Baer, Walter S. *Telecommunications Technology in the 1980's.* Rand Paper Series #P-6275. Santa Monica: Rand Corporation, 1978.

Ball, Desmond. *The Intelligence War in the Gulf.* Canberra, Australia: Strategic and Defense Studies Center, Australian National University, 1991.

Beach, Darrell, and Tommi Selby. Maxwell AFB, Ala., Gunter Annex, SSC/SSF Division, AF Communications Command. Meeting concerning architecture of telecommunications, 8 February 1993.

Bennet, Ralph. *Ultra in the West: The Normandy Campaign, 1944–45*. New York: Charles Scribner's Sons, 1979.

Board on Army Science and Technology Commission on Engineering and Technological Systems National Research Council. *STAR 21: Strategic Technologies for the Army of the Twenty-First Century*. Washington, D.C.: National Academy Press, 1992.

Boyd, John R. *Organic Design for Command and Control.* Maxwell AFB, Ala.: Air University Library, Document M-U 43947-2, May 1987.

Broad, William J. "Russia Is Now Selling Spy Photos From Space." *New York Times*, 4 October 1992, 10.

Brodie, Bernard. *War and Politics*. New York: MacMillan, 1973.

Brown, Anthony C. *Body Guard of Lies*. New York: Harper and Row, 1975.

Builder, Carl H. *The Role of Airpower Theory in the Evolution and Fate of the USAF*. Briefing to SAAS, 10 November 1992.

Bushaus, Dawn. "Hugo No Match for So. Bell." *Telephony*, 25 September 1989, 3.

Calvocoressi, Peter. *Top Secret Ultra.* New York: Pantheon Books, 1980.

Clausewitz, Carl von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Coates, Joseph F. *Nonlethal and Nondestructive Combat in Cities Overseas.* Institute for Defense Analysis, Science and Technology Division, Arlington, Va. Report #DAHC 1567C0011, Task T-62, May 1970.

Cohen, Shelton M. *Arms and Judgement.* Boulder, Colo.: Westview Press, Inc., 1989.

Congress of the United States, Office of Technological Assessment. *Critical Connections: Communications for the Future.* Washington, D.C.: US Government Printing Office, 1990.

Coningham, Air Marshal Arthur. "The Development of Tactical Air Forces." *Royal United Services Institution Journal.* Vol. 91, 1946, 211–226.

Cushman, John H. *Command and Control of Theater Forces: Adequacy.* Washington, D.C.: AFCEA International Press, 1985.

Defense Advanced Research Projects Agency. *Assessment of Mission Kill Concept, Requirements, and Technologies.* Final Report #SPC 1361, SPC Log no. 90-1987, September 1990.

Dateline Television Program Transcript, Affiliate of NBC News. *Are Your Secrets Safe.* Burrelle's Information Service, Box 7, Livingston, N.J. 07039, 27 October 1992.

Debban, Lt Col Alan W. "Disabling Systems: War Fighting Option for the Future." *Airpower Journal* 7, no. 1 (Spring 1993): 44–50.

Defense Intelligence Agency. *Telecommunications Systems—Iraq (U).* Maxwell AFB, Ala.: AU Library, Document no. M-S 41290-963, no. 1720–30, July 1984. Information extracted is unclassified.

Delbruck, Hans. *Warfare in Antiquity.* Lincoln: University of Nebraska Press, 1975.

Department of Defense. *Conduct of the Persian Gulf War*, Final Report to Congress, April 1992.

_____. *Electronic Warfare Threat to U.S. Satellite Communication Links—USSR.* Defense Intelligence Agency, A Defense S and T Intelligence Study, #DST-26105-1-91, 20 March 1991.

Dickens, Adm Gerald. *Bombing and Strategy.* London: Sampson, Low, Marston and Co., 1949.

Doral, Capt Paul R. *Joint Munitions Effectiveness Manuals.* USAF Fighter Weapons School Instructional Text, Courses F4000IOAN, A1000IDOPN, F-1600IDOPN, F-1500IDOPN, Part 1, June 1982.

Doner, John R. et al. *Distributed Network Vulnerability Assessment (DNVA).* Harris Corp., Final Report RADC-TR-89-273. Vol. 1. Griffiss AFB, N.Y.: Rome Air Development Center, Air Force Systems Command, January 1990.

Dordick, Herbert S. *Understanding Modern Communications.* New York: McGraw Hill, 1986.

Douhet, Giulio. *The Command of the Air.* Washington, D.C.: Office of Air Force History, 1983.

Eichen, Mark W., and Jon A. Rochlis. *With Microscope and Tweezers: An Analysis of the INTERNET Virus of Nov 1988*. Cambridge, Mass.: Massachusetts Institute of Technology, 9 February 1989.

Faber, Maj Peter R. "Our Quarrel Is With the Regime, Not the People." Unpublished SAAS Point Paper, 15 September 1992.

Felman, Lt Col Marc D. "The Military/Media Clash and the New Principle of War: Media Spin." SAAS thesis, May 1992.

Foreign Broadcast Information Service. *Soviet Union: Military Affairs Tactics*. Report #JPRS-UMA-88-008-L-1, 29 June 1988.

Fulghum, David A. "Secret Carbon-Fiber Warheads Blinded Iraqi Air Defenses." *Aviation Week & Space Technology*, 27 April 1992.

Fuller, John F. C. *Memoirs of an Unconventional Soldier*. London: Ivor, Nicholson, and Watson Ltd., 1936.

Griffith, Samuel B. *Sun Tzu: The Art of War*. New York: Oxford University Press, 1963.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics 1851–1945*. New York: Oxford University Press, Inc., 1991.

Hill, Ensign Timothy M. *To Stop a Navy: New Ideas for New Threats*. Unpublished Los Alamos National Laboratories Paper, August 1992.

Hopkins, John C. Los Alamos National Laboratories. Memorandum to J. C. Brown in response to a nonlethal strategy group meeting, 20 September 1991.

Howard, Michael. *British Intelligence in the Second World War, Vol V Strategic Deception*. New York: Cambridge University Press, 1990.

Krepinevich, Lt Col Andrew F., Jr. *The Military-Technical Revolution, A Preliminary Assessment*. Washington, D.C.: Office of the Secretary of Defense, Office of Net Assessment, July 1992.

Lewonoski, Lt Col Mark C. "Information War." An essay presented to the Air War College faculty in fulfillment of the curriculum requirement. Maxwell AFB, Ala.: Air University, 1991.

Liddel Hart, Capt Basil H. *Paris or the Future of War*. New York: E. P. Dutton, 1925.

_____. *Strategy*. New York: Meridian, The Penguin Group, 1991.

Mar, Ronald K. "Bangless Tank Killer." *Proceedings*, September 1986.

Martin, James. *Telecommunications and the Computer*. Englewood Cliffs, N.J.: Prentice Hall, 1990.

Martin, Capt Mark D. *Non-Lethal Weapons: A Policy Planning Paper*. Office of the Under Secretary of Defense, Policy Planning Division, 29 May 1991.

Mendelsohn, John. *Covert Warfare: Vol 15, Basic Deception and the Normandy Invasion*. New York: Garland Publishing Inc., 1989.

Morris, David J. *Communications Command and Control Systems.* New York: Pergamon Press, 1977.

Morris, Janet. *In Search of a Nonlethal Strategy.* US Global Strategy Council Point Paper, no date.

_____. Nonlethality Briefing (no title), 1991.

Morris, Chris, and Janet Morris. *Expanding Air/Land/Sea Battle Options with Nonlethal Technologies.* Nonlethality Briefing Supplement #1.

Murray, Williamson. *The Combined Bomber Offensive.* Freiburg: MGFA, 18 March 1992.

_____. "Ultra: Some Thoughts on Its Impact on the Second World War." *Air University Review,* July–August 1984, 52–64.

Operation Short Circuit: Complete Disruption of Telecommunications of the Western German Armies. Historical Research Agency, Maxwell AFB, Ala., File #512.425, 1945.

Overy, R. J. *The Air War 1939–1945.* Chelsea, Mich.: Scarborough House Publishers, 1980.

_____. "Air Power, Armies, and the War in the West, 1940." *The Harmon Memorial Lectures in Military History (No 32), USAF Academy, 1989.* Washington, D.C.: Superintendent of Documents, US Government Printing Office, 1989.

Pape, Robert A. "Coercion and Military Strategy: Why Denial Works and Punishment Doesn't." Published in the SAAS 632 Course Readings. Vol. 4, 1991.

Park, Hays W. "Air War and the Law of War." *The Air Force Law Review*. Vol. 32, no. 1, 1990, 1–225.

_____. "Linebacker and the Law of War." *Air University Review,* January–February 1983, 2–30.

_____. "Rolling Thunder and the Law of War." *Air University Review,* January–February 1982, 2–23.

Putney, Diane T. *Ultra and the Army Air Forces In World War II.* Washington, D.C.: US Government Printing Office, 1987.

Rome Laboratory. *Efficient Network Models.* Final Technical Report #RL-TR-92-65. Griffiss AFB, N. Y.: USAF Systems Command, May 1992.

_____. *Network Vulnerabilities Study.* Final Technical Report #RADC-TR-89-341. Griffiss AFB, N.Y.: USAF Systems Command, January 1990.

Rice, M. A., and A. J. Sammes. *Communications and Information Systems for Battlefield Command and Control.* London: Brassey's (UK), 1989.

Ricks, Thomas E. "New Class of Weapons Could Incapacitate Foe Yet Limit Casualties." *The Wall Street Journal,* 4 January 1993.

Salvaggio, Jerry L. *Telecommunications: Issues and Choices for Society.* New York: Longman,1983.

Schelling, Thomas C. *Arms and Influence.* New Haven, Conn: Yale University Press, 1966.

Secure Solutions, Inc. *Placement of Network Security Services for Secure Data Exchange.* SBIR Topic Number N91-061. La Jolla, Calif.: Secure Solutions, 2 November 1992.

Seversky, Alexander de. "Air Power." Speech delivered to Air University, 28 May 1948.

Stares, Paul B. *Command Performance: The Neglected Dimension of European Security.* Washington, D.C.: Brookings Institution, 1991.

Stephen, Major. *Nuclear Warfare Strategy.* Fact Paper, USCENTCOM Scientific and Technological Branch, 17 March 1992.

Stryker, Daniel. *Cobra.* New York: Jove Publications, 1991.

Tanenbaum, Andrew S. *Computer Networks.* Englewood Cliffs, N.J.: Prentice Hall, 1989.

"The Arsenal of the Future—Weapons Designed Not To Kill." *Army,* December 1992.

"The Intelligence War in the Gulf." *Aviation Week & Space Technology,* 22 April 1991, 79.

Towle, Phillip Anthony. *Pilots and Rebels: The Use of Aircraft in Unconventional Warfare 1918–1988.* London: Brassey's (UK), 1989.

US Army Research Institute for the Behavioral and Social Sciences. *Doing Deception: Attacking the Enemy's Decision Process.* Research Report #1550, February 1990.

US Army Special Operations Command. *Special Operations Targeting Handbook.* Edition VIII, October 1991.

US Space Command. *United States Space Command Operations Desert Shield and Desert Storm Assessment(U)(Secret/NO FORN).* US Space Command, Peterson AFB, Colo., January 1992. Information extracted is unclassified.

United States Strategic Bombing Surveys (European War, Pacific War). Maxwell AFB, Ala.: Air University Press, October 1987.

Walsh, Miguel D. "New Technology, War and International Law." Unpublished Paper, 14 June 1991.

Warden, Col John A. III. A series of air power theory briefings presented to SAAS in the Fall 1992.

_____. *Major Lessons From The Gulf War.* Briefing to SAAS, August 1992.

_____. *The Air Campaign.* Washington, D.C.: National Defense University Press, 1988.

Weinschenk, Andrew. "Army Gives a Boost to Exotic, Non-Lethal Weapons." *Defense Week* 13, no. 41, 19 October 1992, 1 and 9.

Welchman, Gordon. *The Hut Six Story: Breaking the Enigma Codes.* New York: McGraw Hill Book Co., 1982.

Winterbotham, F. W. *The Ultra Secret.* New York: Harper and Row, 1974.